



Homeland
Security

February 5, 2020

Mark J.F. Schroeder
Acting Commissioner
New York State Department
of Motor Vehicles
6 Empire State Plaza
Albany, NY 12228
mark.schroeder@dmv.ny.gov

Theresa L. Egan
Executive Deputy Commissioner
New York State Department
of Motor Vehicles
6 Empire State Plaza
Albany, NY 12228
theresa.egan@dmv.ny.gov

Via email and U.S. mail

Dear Mr. Schroeder and Mrs. Egan:

On June 17, 2019, the State of New York (New York) enacted the Driver's License Access and Privacy Act (the Act), effective December 14, 2019.¹ The Act forbids New York Department of Motor Vehicles (DMV) officials from providing, with very limited exceptions, pertinent driver's license and vehicle registration information to the United States Department of Homeland Security (DHS). Specifically, this Act precludes U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) from accessing and validating pertinent information contained in New York DMV records that is operationally critical in DHS's efforts to keep our Nation secure. The Act also threatens to block access to other state law enforcement agencies and departments if those agencies or departments provide New York DMV records to CBP and ICE.

Over the years, CBP has utilized New York DMV records in several ways to promote national security and to enforce federal customs and immigration laws. Having access to New York DMV information has enabled CBP to validate that an individual applying for Trusted Traveler Programs (TTP) membership qualifies for low-risk status or meets other program requirements. An individual's criminal history affects their eligibility for TTP membership. TTP permits expedited processing into the United States from: international destinations (under Global Entry); Canada only (under NEXUS); and Canada and Mexico only (under SENTRI). TTP also allows quicker processing for commercial truck drivers entering or exiting the United States (under FAST). Furthermore, CBP has needed New York DMV records to establish ownership and thus to determine whether a used vehicle is approved for export.

¹ N.Y. Veh. & Traf. § 201 (2019).

The Act prevents DHS from accessing relevant information that only New York DMV maintains, including some aspects of an individual's criminal history. As such, the Act compromises CBP's ability to confirm whether an individual applying for TTP membership meets program eligibility requirements. Moreover, the Act delays a used vehicle owner's ability to obtain CBP authorization for exporting their vehicle.

Furthermore, on a daily basis, ICE has used New York DMV data in its efforts to combat transnational gangs, narcotics smuggling, human smuggling and trafficking, trafficking of weapons and other contraband, child exploitation, exportation of sensitive technology, fraud, and identity theft. In New York alone, last year ICE arrested 149 child predators, identified or rescued 105 victims of exploitation and human trafficking, arrested 230 gang members, and seized 6,487 pounds of illegal narcotics, including fentanyl and opioids.² In the vast majority of these cases, ICE relied on New York DMV records to fulfill its mission. ICE also needs New York DMV information to safeguard Americans' financial and intellectual property rights.

New York DMV records have long been used by ICE law enforcement personnel to verify or corroborate an investigatory target's Personally Identifiable Information (PII), which can include their residential address, date of birth, height, weight, eye color, hair color, facial photograph, license plate, and vehicle registration information. Moreover, ICE's expeditious retrieval of vehicle and driver's license and identification information has helped identify targets, witnesses, victims, and assets. ICE has used DMV records to obtain search warrants, and DMV records are also critical for ICE to identify criminal networks, create new leads for investigation, and compile photographic line-ups. Additionally, during the execution of search and arrest warrants, ICE officers have used DMV information to identify individuals whose criminal history renders them a threat. The Act prohibits the sharing of vehicle registration information, including the identity of the person to whom the vehicle is registered, with DHS. That prohibition prevents ICE from running license plate searches, even when ICE is aware that the vehicle's owner has committed a heinous crime. In short, this Act will impede ICE's objective of protecting the people of New York from menacing threats to national security and public safety.

Although DHS would prefer to continue our long-standing cooperative relationship with New York on a variety of these critical homeland security initiatives, this Act and the corresponding lack of security cooperation from the New York DMV requires DHS to take immediate action to ensure DHS's efforts to protect the Homeland are not compromised.

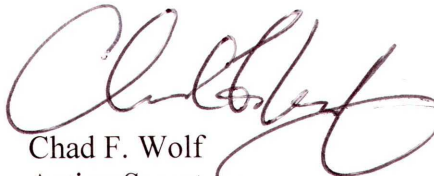
² Nationwide, last year ICE arrested nearly 4,000 child predators, identified or rescued 1,400 victims of exploitation and trafficking, arrested 3,800 gang members, and seized 633,000 pounds of contraband, including fentanyl and opioids.

Due to the Act's negative impact on Department operations, DHS will immediately take the following actions:

- (1) **Trusted Traveler Programs—Global Entry, NEXUS, SENTRI, and FAST.** Because the Act prevents DHS from accessing New York DMV records in order to determine whether a TTP applicant or re-applicant meets program eligibility requirements, New York residents will no longer be eligible to enroll or re-enroll in CBP's Trusted Traveler Programs.
- (2) **Vehicle Exports.** Because the Act hinders DHS from validating documents used to establish vehicle ownership, the exporting of used vehicles titled and registered in New York will be significantly delayed and could also be costlier.

These actions are the result of an initial assessment conducted by DHS. We will continue to review Department-wide operations related to New York to assess and mitigate the Act's adverse impact on national security and law enforcement.

Sincerely,




Chad F. Wolf
Acting Secretary



Homeland Security

December 30, 2019

MEMORANDUM FOR OPERATIONAL COMPONENT HEADS

FROM: Chad F. Wolf 
Acting Secretary

SUBJECT: Operational Assessment of State Laws Restricting the Sharing of
Department of Motor Vehicle Information with DHS

Purpose

Certain state legislatures have passed laws restricting their respective Department of Motor Vehicles ("DMV") agencies from sharing information with the Department. These laws may detrimentally impact the ability of the Department to perform our security-related missions. Accordingly, I am instructing each operational component to conduct an assessment of the impact of these laws, so that the Department is prepared to deal with and counter these impacts as we protect the homeland.

Background

On June 17, 2019, New York enacted the Driver's License Access and Privacy Act, also known as the "Green Light Law." The law took effect on Monday, December 16, 2019. The Green Light Law prohibits disclosing or making accessible "records or information" for license applicants and holders to federal immigration authorities absent a court order or judicial warrant from an Article III judge. The law also requires notice to individuals who are subject to information/records requests from immigration authorities.

Other states have enacted similar laws. For example, on December 19, 2019, the Governor of New Jersey signed a law that places similar restrictions on the sharing of DMV information with federal immigration authorities.¹ Additionally, there are other states that restrict the sharing of DMV information with federal authorities. Due to the enactment of state laws that directly impact the ability of states to cooperate with law enforcement, and DHS in particular, it is necessary for a Department-wide assessment of the impacts that these laws create and the potential solutions to mitigate any impacts.

¹ The New Jersey law will become effective in January, 2021.

Subject: Operational Assessment of State Laws Restricting the Sharing of Department of Motor Vehicle Information with DHS

Page 2

Operational Assessment

To determine the operational impact created by state laws that limit or prohibit the sharing of DMV information with the Department, each Operational Component shall conduct an operational assessment outlining the impacts to Department missions that flow from these information-sharing restrictions.

The operational assessments should include answers to the following questions:

1. What DMV information is currently available to your Component and how is it accessed? Components should identify each state and territory that currently restricts access to DMV information.
2. How is DMV information used in the day-to-day operations of your Component?
3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?
4. What are the long-term operational impacts of not having access to DMV information?
5. Are there alternative ways to obtain the information contained in the DMV databases?
6. What are the short-term and long-term solutions available to address the security consequences, if any, that result from losing access to DMV information?

The Office of Strategy, Policy, and Plans (Policy) will coordinate the development of these assessments with the Operational Components, consolidate each of the assessments into a single Department-wide assessment, and provide me with recommended courses of action to address any identified impacts associated with these state laws. Policy shall provide me with the consolidated assessment by January 15th.

As Operational Components conduct these assessments, it should in no way impede or delay any action to implement appropriate mitigation measures to ensure the safety and security of the American people.

For Official Use Only

U.S. Customs and Border Protection State of New York's "Green Light Law" December 30, 2019

Issue: Passage of the New York (NY) "Green Light Law," has resulted in the denial of U.S. Customs and Border Protection (CBP) access to NY Department of Motor Vehicles (DMV) records via the National Law Enforcement Telecommunications System (NLETS). The denial includes data relating to state-issued identification documents, including driver's licenses, as well as vehicle registrations and license plates. CBP uses NLETS for a variety of reasons beyond immigration enforcement. The State of NY information is used for national security and enforcement of agricultural and Customs laws as well as other federal laws that CBP enforces and administers at the border. In addition, travelers and stakeholders routinely present NY-issued documents to CBP such as driver's licenses, registration, and license plates, in the course of normal business operations. The inability of CBP to validate against NY state databases, through NLETS, impacts the following areas:

Targeting and Operations:

- Validating NY vehicle license plates and registration to determine the associated risk of, and to target for more fulsome inspections, vehicles crossing at ports of entry, roving Border Patrol vehicle stops, and at Border Patrol checkpoints.
 - Increases vulnerability to smuggling and other cross-border violations, as well as officer safety concerns.
- Targeting national security risks, criminals, and registered sex offenders, including child sex offenders, who are residents of NY.
- Mitigating and conducting analysis of high-risk cargo shipments with a nexus to the State of NY.

Trusted Traveler Programs (TTP):

- Validating NY driver's licenses presented as part of the interview process for issuance of the TTP cards. TTP cards serve in lieu of a passport at land borders. NEXUS cards in particular are Western Hemisphere Travel Initiative (WHTI) compliant documents for travel by land, the marine environment, and air (departure from CBP Canadian Pre-Clearance locations).

Vehicle Exports:

- Determining the authenticity of a vehicle title and/or owner information. Retrieval of registration and lien data is performed at inspection in accordance with 19 CFR 192.2.

Fines Penalties and Forfeitures:

- Determining the titled owner of seized vehicles to ensure the notice of seizure is issued according to law.

For Official Use Only

For Official Use Only

Passenger Processing:

- Confirming the validity of NY Enhanced Driver's Licenses (EDLs) in our secondary environments, with potential near-term impact upon such confirmations at primary inspection.
- Confirming a traveler's identity in the passenger environment when the validity of a passport or other identify document is in question.
- Confirming vehicle ownership.
- Enhancing intelligence information when identifying individuals associated to illicit activities.
- Confirming identity by cross-reference to other databases.
- Conducting queries for research on specific individuals of concern.

Administrative Security:

- Verifying NY identification documents required for the issuance of Customs Seals for access to Federal Inspection Service Areas at airports and warehouses.

Task Forces:

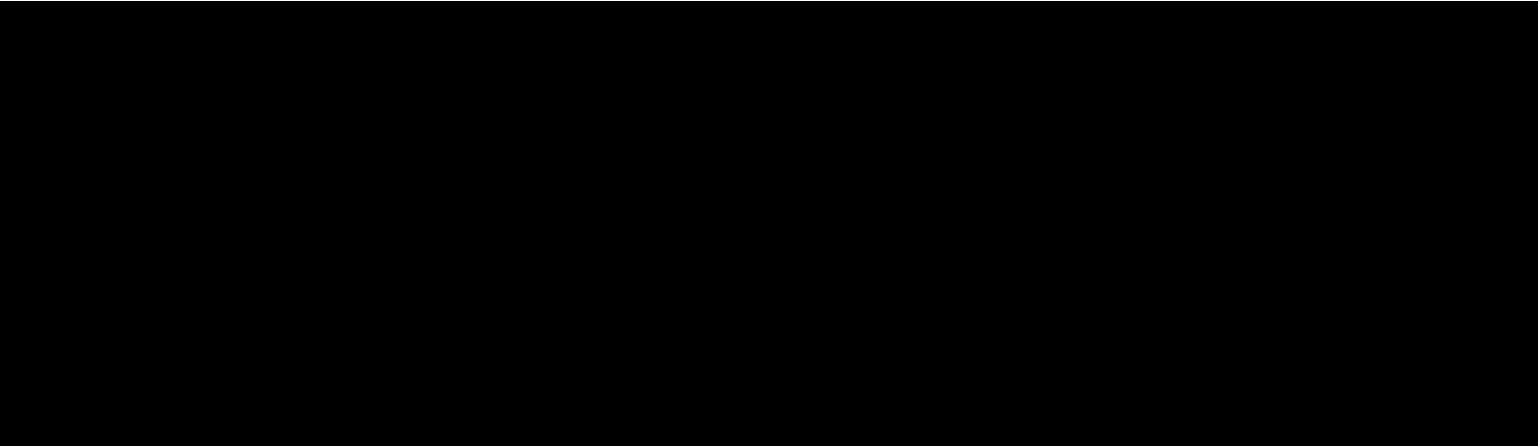
- Determining the registered owner of a vehicle with NY license plates during joint investigations and operations, and counter-terrorism responses with law enforcement partners (except to the extent that information sharing continues from NY state to Task Force partners other than CBP and ICE).
- Limiting the sharing of NY DMV information with CBP and ICE, which complicates and hinders full CBP participation in Task Forces.

Employment:

- Conducting all required checks necessary for background investigations, periodic reinvestigations, and continuous evaluations.
 - Those investigations help determine suitability and eligibility for employment, and their adjudication requires all information related to criminal history, driving offenses, traffic citations, etc. The biggest concerns surround the potential lack of information regarding DUI/DWIs. Some jurisdictions capture those offenses as traffic citations rather than criminal offenses, and would not be listed in NCIC. The risk to the agency is that we would not have complete information to make determinations regarding suitability for employment.

For Official Use Only

For Official Use Only



For Official Use Only




U.S. Customs and
Border Protection

Commissioner

JAN 08 2020

DECISION

MEMORANDUM FOR THE ACTING DEPUTY SECRETARY

FROM: Mark A. Morgan 
Acting Commissioner

SUBJECT: New York "Green Light Law" – Implications and
Recommendations

Purpose: This memorandum seeks your approval for the below recommendations to address the security vulnerabilities created by the State of New York's "Green Light Law" that restricts U.S. Customs and Border Protection's (CBP) access to New York (NY) Department of Motor Vehicles (DMV) data. CBP first recommends engaging with the State of NY to resolve the restricted access prior to implementing any of the recommendations identified below.

Background: Due to the passage of the NY Driver's License Access and Privacy Act ("Green Light Law"), CBP access to NY DMV records via the National Law Enforcement Telecommunications System (NLETS) has been discontinued and other entities that receive NLETS data will be required to certify that they will not share NLETS data with CBP (and U.S. Immigration and Customs Enforcement (ICE)) resulting in a complete denial of this information to CBP. The denial includes data relating to state-issued identification documents, including driver's licenses, as well as vehicle registrations and license plates. CBP uses NLETS for a variety of reasons beyond immigration enforcement. The State of NY information is used for national security, enforcement of agricultural and customs laws as well as other federal laws that CBP enforces and administers at the border. In addition, travelers and stakeholders routinely present NY-issued documents to CBP such as driver's licenses, registration, and license plates, in the course of normal business operations. At this time, CBP continues to receive DMV data from other states who have restricted access to ICE.

Broad authorities enable CBP to meet its mission responsibilities, as articulated in 6 U.S.C. § 211. Information received from federal, state, local, tribal, and territorial partners is essential to CBP's law enforcement efforts, and particularly to CBP's ability to "develop and implement screening and targeting capabilities, including the screening, reviewing, identifying, and prioritizing of passengers and cargo across all international modes of transportation, both inbound and outbound." See 6 U.S.C. § 211(c)(9) (outlining duties of the Commissioner); 6 U.S.C. § 211(g)(4)(C) (charging the National Targeting Center with the duty "to collect and analyze traveler and cargo information in advance of arrival in the United States to identify and

address security risks... [and] identify, review, and target travelers and cargo for examination...”).¹

Discussion: The inability of CBP to validate information, such as driver’s license and registration, against the NY state databases, through NLETS, impacts multiple CBP activities, as outlined below.

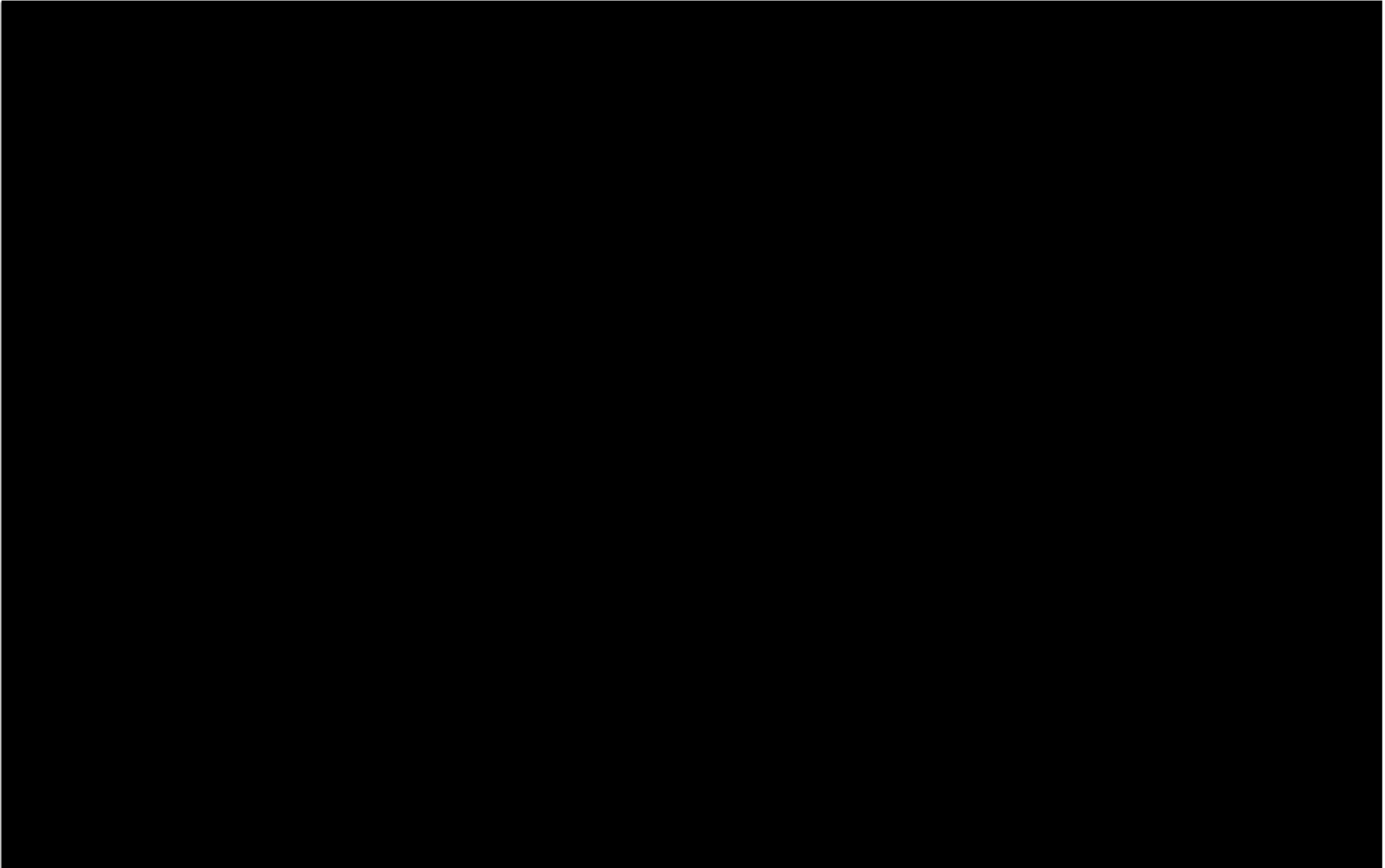
Passenger Processing

Trusted Traveler Programs (TTP):

- Approximately 9.5 million travelers are currently enrolled in CBP’s four TTPs:
 - Global Entry (6.9 million members), which allows expedited air arrival processing for pre-approved, low-risk air travelers;
 - NEXUS (1.9 million members), allowing pre-screened U.S. and Canadian citizens expedited processing when entering the United States by land and Canada by air or land;
 - The Secure Electronic Network for Travelers Rapid Inspection (SENTRI) Program (552K members), allowing expedited clearance for pre-approved, low-risk travelers at southern U.S. land border ports; and
 - The Free and Secure Trade (FAST) Program (76K members), a commercial clearance program for known low-risk commercial shipments entering the United States from Canada and Mexico.
- These programs expedite the processing of known, low risk, vetted travelers arriving into the United States, permitting CBP officers additional time to focus on higher risk, unknown travelers.
- Identity confirmation is a critical element in establishing eligibility to participate in any of CBP’s TTPs. NLETS enables CBP to validate NY driver’s license identity during the


¹ **Authorities:** CBP officers have the authority to board conveyances, including vehicles, crossing the border; examine the cargo and contents of such vehicles; examine records and documents regarding such vehicles, their occupants, and their contents; demand assistance in carrying out its law enforcement authorities; and issue penalties or pursue seizure and forfeiture for violations. *See e.g.*, 8 U.S.C. § 1357 (general enforcement authorities, including authority to take and consider evidence); 19 U.S.C. § 482 (broad authority to search, including to search vehicles); 19 U.S.C. § 507 (“authority to demand the assistance of any person in making any arrest, search, or seizure authority by any law enforced or administered by customs officers”); 19 U.S.C. § 535 (compulsory production of books, invoices, or papers); 19 U.S.C. § 1431 (manifest requirements); 19 U.S.C. § 1436 (providing for penalties); 19 U.S.C. § 1454 (providing for penalties); 19 U.S.C. § 1455 (boarding vessels and vehicles and examining the cargo and contents thereof, and providing for penalties); 19 U.S.C. § 1459 (reporting requirements for individuals, including individuals arriving by unreported conveyance, and providing for penalties for violations); 19 U.S.C. § 1462 (forfeiture); 19 U.S.C. § 1509 (examination of books and witnesses); 19 U.S.C. § 1581 (authorizing customs officers to “examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board, and to this end may hail and stop such vessel or vehicle, and use all necessary force to compel compliance” and providing for penalties for noncompliance); 19 U.S.C. § 1584 (penalties for falsity or lack of manifest for “the person in charge of such vehicle or the owner of such ... vehicle”); 19 U.S.C. § 1589a (law enforcement authority); 19 U.S.C. § 1594 (seizure of conveyances); 19 U.S.C. § 1607 (notice of seizure for articles valued under \$500,000, prohibited articles, and transporting conveyances); 19 U.S.C. § 1646c (reporting requirements for persons or entities exporting used automobiles).

interview process for issuance of the TTP cards which serve in lieu of a passport at land borders.

- More than [REDACTED] NY residents are CBP TTP members and over [REDACTED] NY residents have a TTP application pending vetting.
 - In calendar year 2019, NY state residents who are TTP members have entered the U.S. via the northern land border more than [REDACTED] times and arrived via air into the NY state area more than [REDACTED] times.
 - In 2019, a total of [REDACTED] NY licensed drivers utilized FAST lanes to cross the northern land border a total of [REDACTED] times.
- 

Enhanced Driver's License (EDL) Program:

- State-issued EDLs provide proof of identity and U.S. citizenship, are issued in a secure process, and include technology that makes travel easier.
 - They provide travelers with a low-cost, convenient alternative for entering the United States from Canada, Mexico or the Caribbean through a land or sea port of entry, in addition to serving as a permit to drive.
 - The Department has been working with states to enhance their driver's licenses and identification documents to comply with travel rules under the Western Hemisphere Travel Initiative (WHTI), effective June 1, 2009.

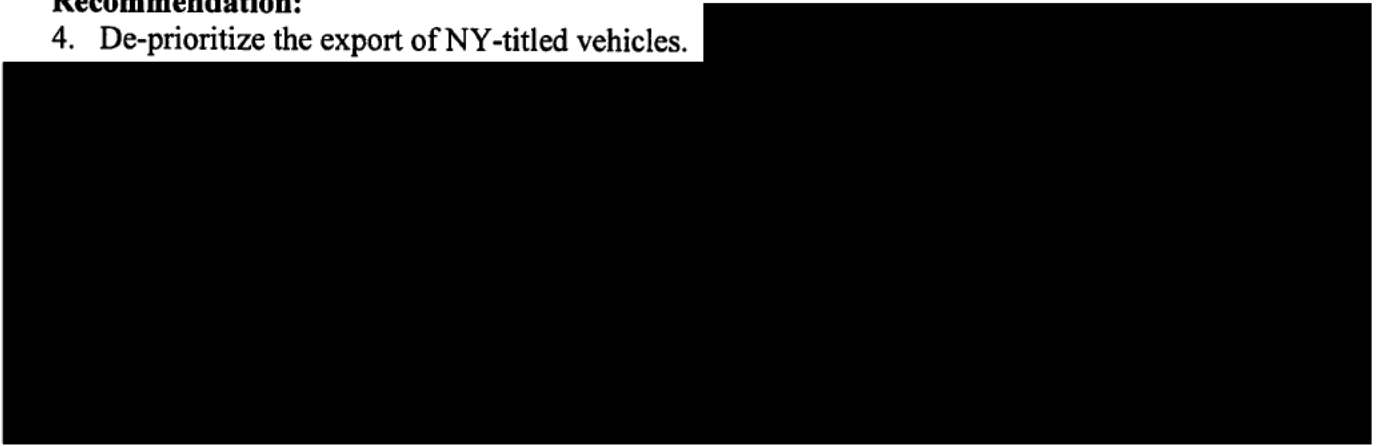
- Currently, DHS is party to a memorandum of agreement (MOA) between the NY DMV and DHS which allows CBP to validate a traveler’s identity and citizenship utilizing EDLs.
 - The MOA provides that either party may terminate the MOA by providing written notice thirty (30) calendar days in advance of the termination.
 - While NY has not notified CBP of an intention to terminate the MOA, there is a strong likelihood that NY will withdraw from the MOA in light of the Green Light Law. If that happens, and the State of NY prevents CBP’s access to driver’s license and registration data, CBP will no longer be able to validate a traveler’s identity with the EDL.
 - Given that approximately 2.3 million NY EDLs have been issued, this will have an operational impact.
 - In FY 2019, there were approximately [REDACTED] NY EDL crossings nationally with an average of [REDACTED] per day. The highest three volume locations for NY EDLs [REDACTED] saw up to [REDACTED] NY EDL crossings in the busiest month being August 2019, more than [REDACTED] per day in these locations alone.
- 

Vehicle Exports:

- CBP must determine eligibility of vehicles titled in NY, specifically to verify clear ownership of the vehicle by the exporter.
- Retrieval of registration and lien data is performed at inspection in accordance with 19 C.F.R. §192.2 which requires the advance submission and authentication by CBP of both the vehicle and supporting documentation, in this case a U.S. issued certificate of title.
- CBP estimates that there were approximately [REDACTED] vehicles exported in 2019 with NY titles. Without access to NY DMV NLETS data CBP is required to manually authenticate the vehicle and supporting data.

² See 8 CFR 235.1(d) (“The Secretary of Homeland Security will announce, by publication of a notice in the Federal Register, documents designated under this paragraph” concerning enhanced driver’s licenses). This provision likely requires an FRN not only for initial designation, but also for removal from the list.

Recommendation:

4. De-prioritize the export of NY-titled vehicles.
- 

1. What DMV information is currently available to your Component and how is it accessed?

In order to be eligible for certain types of disaster assistance, an individual may be asked to provide documentation distributed by a DMV, such as a driver's license, to prove identity or automobile title to demonstrate vehicle ownership. However, FEMA does not currently have any information-sharing agreement or procedure in place with any DMVs which would be impacted by laws such as those mentioned in the "Operational Assessment of State Laws Restricting the Sharing of Department of Motor Vehicle Information with DHS" memorandum.

2. How is DMV information used in the day-to-day operations of your Component?


Applicants must provide documentation or an inspector must be able to visually verify that their disaster-damaged car was registered prior to the disaster. No information is provided directly by a state or territory DMV.

3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?

There are no current consequences.

4. What are the long-term operational impacts of not having access to DMV information?

Through the Other Needs Assistance provision of FEMA's Individuals and Households Program, FEMA may provide financial assistance to individuals and households with disaster-caused vehicle repair or replacement expenses. This type of assistance, known as Transportation Assistance, was the subject of a Department of Homeland Security's (DHS) Office of Inspector General (OIG) audit which was published in September 2019. In the audit (OIG-19-66-Audit), DHS-OIG reported that FEMA did not sufficiently safeguard the use of Transportation Assistance funds, specifically stating that FEMA's policies and procedures do not require documenting comprehensive insurance and second vehicle verification. In its recommendations for corrective action, DHS-OIG proposed that FEMA ensure future information technology updates support the collection, use, and retention of unique Vehicle Identification Numbers to enable FEMA to cross-reference national databases (such as DMVs) to confirm insurance coverage and identify applicants' second vehicles.



5. Are there alternative ways to obtain the information contained in the DMV databases?

FEMA could continue current practices requiring applicants to provide their own documentation, but we would not be able to cross reference state, territory, or national databases to confirm car insurance coverage or vehicle ownership.

6. What are the short-term and long-term solutions available to address the security consequences, if any, that result from losing access to DMV information?

As Individual Assistance does not currently use this information, additional research would be required to identify methods to verify applicant's self-reporting of car insurance coverage, number of vehicles owned, and any potential follow-up to ensure destroyed cars are not resold.

Subject: TSA-191231-3: AS1 memo to Operational Components

1. What DMV information is currently available to your Component and how is it accessed?

Components should identify each state and territory that currently restricts access to DMV information.

Answer: The Transportation Security Administration (TSA) does not directly access DMV systems for any information, including for the vetting of airline passengers or credentialing applicants. TSA accesses various Federal databases and may rely on commercial sources to confirm an individual's information which is ordinarily provided by an individual in the first instance. These databases and sources include National Law Enforcement Telecommunications System (NLETS), National Commercial Driver's License Information System (CDLIS) and Lexis Nexis.

NLETS is a law enforcement sharing database where data is shared through the individual state. CDLIS is a nationwide computer system that enables state driver licensing agencies to ensure that each commercial driver has only one driver's license and one complete driver record. CDLIS contains mostly the same information as NLETS, but will often have the date of issue for driver's licenses.

[REDACTED]

2. How is DMV information used in the day-to-day operations of your Component?

Answer: As stated above, TSA does not directly access DMV systems in the course of vetting airline passengers or credentialing applicants. TSA accesses various Federal databases and may rely on commercial sources to confirm an individual's information which is ordinarily provided by an individual in the first instance. TSA uses these sources to validate the driver's license information of an airline passenger or credential applicant and/or de-conflict a name found on a watchlist or other derogatory information, such as criminal history or national security vetting sources.

3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?

Answer: TSA does not know whether the accuracy of [REDACTED]

[REDACTED]

4. What are the long-term operational impacts of not having access to DMV information?

Answer: As stated above, TSA does not have knowledge of [REDACTED]

[REDACTED]

[REDACTED]

5. Are there alternative ways to obtain the information contained in the DMV databases?

Answer: As previously mentioned, TSA does not directly access DMV systems in the course of vetting travelers or credential holders. TSA accesses various Federal databases and may rely on commercial sources to confirm an individual's information which is ordinarily provided by an individual in the first instance. [REDACTED]

6. What are the short-term and long-term solutions available to address the security consequences, if any, that result from losing access to DMV information?

Answer: TSA does not directly access DMV systems in the course of vetting travelers and credential holders. However, TSA has subpoena authority that can be exercised when there is a particular need for an individual's information in a DMV system. TSA vetting and adjudication operations will continue to access Federal databases and commercial sources that collect and aggregate data for mission related purposes.



U.S. Immigration and Customs Enforcement Response to Operational Assessment of State Laws Restricting the Sharing of Department of Motor Vehicle Information with DHS

January 14, 2019

1. What DMV information is currently available to ICE and how is it accessed?

A. What DMV information is currently available to ICE ?

Department of Motor Vehicles (DMV) records include information about registered vehicles and individuals who have been issued driver's licenses. Vehicle information may include vehicle identification number, current and prior license plate number(s), vehicle make/model/year/color, vehicle type, lienholder information, and the name and address of current and prior registered owner(s). Driver's license information may include the license holder's name, address, photograph, license status, height and weight, hair and eye color, gender, license number, social security number, and date of issuance/expiration.

B. How is it accessed?

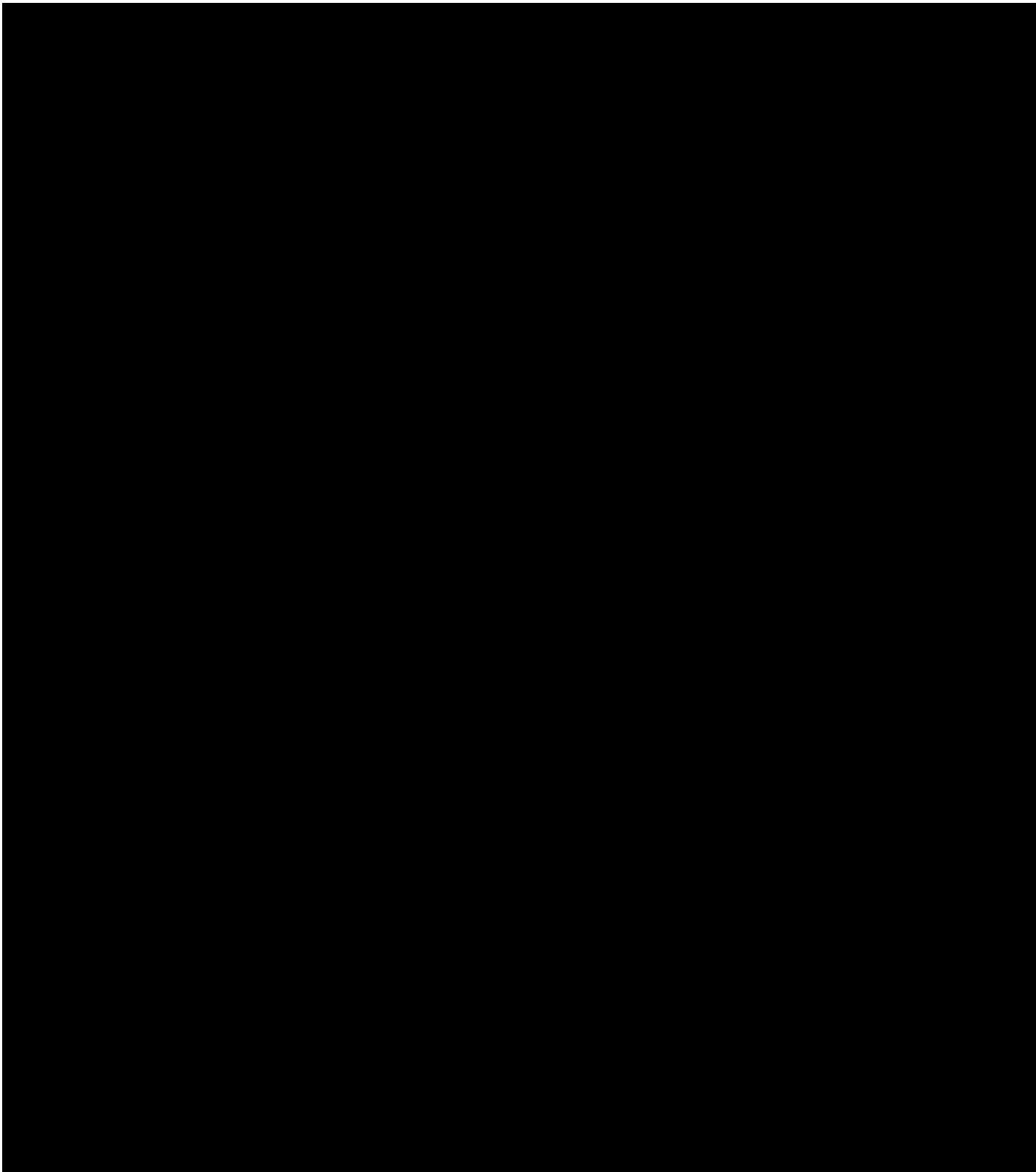
Generally, DMV information is retrieved through the National Law Enforcement Telecommunication System (Nlets) which is accessed through the Customs and Border Protection (CBP) TECS system or the ICE Homeland Security Investigations (HSI) Investigative Case Management (ICM) system. Some states do not participate in Nlets, therefore methods for obtaining DMV information vary in those states. For example, some states provide direct access to their databases through an online portal, some provide ICE with stand-alone terminals located directly at the ICE office, some states direct ICE to obtain data through their local fusion centers, through state and local partners, or through court orders. The DMV information available to ICE also varies from state to state.

Restricted Access

- New York: New York has blocked U.S. Immigration and Customs Enforcement (ICE) by ORI codes, and has instructed all law enforcement agencies/departments with access that providing New York DMV records to ICE will result in a loss of access to their agency. A limited number of HSI New York agents have access to NY DMV data through an e-portal system called E-justice, however this is only available to HSI NY agents and does not alleviate the issue of access for HSI around the country where a majority of NY Nlets queries come from.

- [REDACTED]

FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE



FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE



2. How is DMV information used in the day-to-day operations of ICE?

- a. HSI: ICE HSI uses DMV information on a day-to-day basis to identify, locate, and associate individuals, vehicles, and locations as part of ongoing investigations covering the full range of ICE HSI investigative categories including, but not limited to: narcotics smuggling, child exploitation, human smuggling and trafficking, trans-national gangs, national security, identity and benefit fraud, financial, and intellectual property rights. DMV information is often used to verify or corroborate Personally Identifiable Information (PII) associated with an individual, which can include residential address, date of birth, height, weight, eye color, hair color, a facial photograph, and license plate/vehicle registration information. DMV information can be factual evidence used in affidavits as supporting evidence for residency needed to acquire a judge's signature on federal search warrant applications. It is also critical for building out criminal networks and creating new leads for investigation.

DMV photograph information is used to compile photograph line ups to be used in the field or during interviews, and while conducting facial recognition searches to identify individuals or targets. Furthermore, license plate number identification is used in tracking with both automated license readers and physical surveillance.

The ability to retrieve vehicle and driver's license/identification information in near real-time assists in identifying possible targets, witnesses, victims, and assets, and deconflicting with other local, state, and federal law enforcement agencies. DMV information is crucial to officer safety prior to the execution of an arrest or search warrant by identifying individuals inside the residence of a target of investigation who might pose a threat based on criminal history or other factors.

- b. ERO: State DMV information is used to query driver license history/issuance, vehicle registration history/issuance, and incident/accident reports, and cross reference for



other investigative leads during encounters of suspected foreign-born nationals. The ICE Enforcement and Removal Operations (ERO) Targeting Operations Division (TOD) uses driver's license/DMV searches in varying ways to establish targetability, confirm identity and residence, and determine other relevant information, such as a subject's last known location. This is used to develop target packages used by the 24 field offices to locate criminal aliens and make interior arrests.

ICE ERO officers would also use this information to review and verify a subject's identity against DHS indices. The loss of the ability to corroborate a subject's identity/identities using driver's license information compromises officer safety while enabling persons to evade detection with false or fraudulent ID information.

- c. OPR: The ICE Office of Professional Responsibility (OPR) investigates criminal violations across the full spectrum of the federal code, to include allegations of public corruption, and access to DMV information significantly impacts ICE OPR's ability to protect the homeland and enforce federal criminal laws. ICE OPR routinely uses DMV information and/or photos while conducting criminal investigations to identify and locate suspects, witnesses, victims of crime, and assets that may be subject to seizure.

Additionally, from a personnel security standpoint, while conducting criminal inquiries on ICE applicants, ICE OPR obtains Nlets and DMV information. The DMV information is used to determine if an inordinate number of traffic violations have occurred within given timeframes, as many of ICE's law enforcement positions require the operation of a government owned vehicle on a routine basis. ICE OPR also obtains TECS hits involving suspected drug smuggling operations that may be related to an ICE applicant. These TECS hits usually contain vehicle information, and ICE OPR uses the vehicle information to conduct vehicle registration inquiries through the appropriate state in order to ascertain if the registered vehicle correlates to the applicant in question.

3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?

- a. HSI: If DMV information were not available to ICE HSI investigations, it would be extremely difficult to quickly identify criminal suspects and unnecessarily prolong investigations potentially putting victims, the general public and agents at risk. This is especially crucial in crimes involving child exploitation and human trafficking. Additionally, the inability to quickly access an individual's criminal history, warrant status, or an armed/dangerous alert could unnecessarily endanger agents in the field. Limiting or eliminating access to DMV information could also increase incidents of interfering with other ongoing local, state, and federal criminal investigations.



Numerous state DMVs maintain firearms registration information. The loss of access to firearms registry information also presents a serious impediment to officer safety.

For example, several high-profile acts of domestic terror have recently occurred in the New Jersey / New York area. Access to New Jersey and New York DMV information is imperative to ensure officer and public safety.

- On December 10, 2019, over several hours, two individuals executed a Jersey City, New Jersey Police Officer, killed three other people in Jersey City, New Jersey, and shot at law enforcement, including ICE HSI personnel.. In their rented U-Haul were two pipe bombs. One of the subject's also owned another vehicle that was not immediately located. ICE HSI Newark personnel on-site attempted to query New York DMV for this license plate but were restricted from accessing it.
 - On December 19, 2019, the New York State Office of General Counsel (NYSOGC) contacted ICE HSI Newark regarding a New York DMV system query that was run out of the ICE HSI Newark Field Office. NYSOGC informed ICE HSI Newark that, pursuant to recently-enacted legislation, all access by ICE, U.S. Customs and Border Protection, and U.S. Citizenship and Immigration Services (USCIS) was terminated. In addition, within 3 days of the query, NYS was bound by the new law to notify the individual that ICE ran their information.
 - On December 28, 2019, an individual in Monsey, New York, illegally entered a Synagogue and began to stab the congregants. Five people were stabbed, one critically. The subject fled, but a witness was able to provide license plate information which was then disseminated to the New Jersey/New York law enforcement community. ICE HSI personnel attempted to query the license plate information but were unable to due to state restrictions. ICE HSI personnel requested that an ICE HSI Task Force officer obtain the information and the information was returned in 1.5 hours. The subject was eventually stopped in New York City with the assistance of license plate recognition technology.
- b. ERO: ICE ERO investigations and operations are impeded if the case relied upon these database leads to establish probable cause. The TOD's inability to return DMV data will have a direct impact to officer safety, as the division will be unable to corroborate identity using driver's license information. This could enable persons to fraudulently use other identities to evade detection. In addition, decreased information and data-sharing between state and local DMV entities and the TOD would produce the following impacts:
- lost access to standard driver license, vehicle queries, and criminal history specific to the state;



- inability to access DMV information to assist with at large sex offender investigations;
 - inability to access DMV information to assist with at large aggravated felon investigations;
 - inability to access DMV information to assist with at large Egregious Public Safety (EPS) investigations referred by USCIS;
 - inability to access DMV information to assist with at large Interpol fugitive investigations; and
 - inability to access DMV information to assist with at large criminal alien investigations.
- c. OPR: Limiting or providing no access to critical information, such as a subject's photograph, last known address, physical attributes, and vehicle registration information, can pose serious officer safety risks to law enforcement officers engaging in operational activities. Time-sensitive circumstances require direct and immediate access to DMV data in order to mitigate potential life-threatening situations.

As well, without the ability to obtain state DMV information, ICE risks having personnel security make favorable suitability and national security determinations on applicants who have suspended/revoked drivers licenses. Furthermore, without the ability to verify vehicle registration information, ICE would be restricted in obtaining valuable information that is critical in making sound suitability and national security determinations.

4. What are the long-term operational impacts of not having access to DMV information?

- a. HSI: Long-term loss of DMV information would severely impede ICE HSI's ability to identify, locate, and arrest individuals violating federal law and severely hinder ICE HSI's ability to investigate, disrupt, and dismantle transnational criminal organizations in every case category ICE HSI investigates, resulting in fewer arrests, wasted resources, and a diminished number of otherwise successfully resolved investigations.

[REDACTED] The absence of readily available and reliable DMV information will increase the risk of prematurely exposing sensitive investigations due to the necessity of using alternate methods to identify the identical information contained in DMV records.

ICE HSI agents also rely upon DMV information in affidavits for federal and state search warrants and arrest warrants. A key legal requirement of these documents is that the agent identify the place and person to be searched or arrested. This is



accomplished by running driver's and vehicle information and cited as such in the affidavits. A commonly accepted law enforcement method of identifying an individual is to match an individual or their car to their driver's license. Additionally, DMV information allows the agent to determine if the individual is the subject of an outstanding arrest warrant (to include those issued by state and county agencies). Without this information, agents may encounter wanted criminals and release them.

- b. ERO: ICE ERO identification, arrest, detention, and removal of high priority foreign born nationals will be negatively impacted. The TOD will lose a large amount of data that is currently used to determine the current and last known addresses of criminal aliens, including egregious offenders, gang members, national security threats, and recidivist criminals. Absent this information, the TOD will be unable to build target packages for the field, significantly limiting the number of interior arrests ICE ERO will be able to make on an annual basis. This will have resultant negative impacts on public safety and national security.
- c. OPR: The long-term impact of not having access to DMV information would result in inefficiencies or delays in identifying and locating targets and victims of criminal investigations, as well as law enforcement operations and surveillance during ICE OPR investigations. Furthermore, any restriction in obtaining DMV or Nlets information would have immense consequences in ICE making sound suitability and national security determinations on applicants. These restrictions would continue to compound the longer the restrictions were place, which would result in numerous applicants being allowed to work for ICE that would have otherwise been found ineligible for employment.

5. Are there alternative ways to obtain the information contained in the DMV databases?

- a. HSI: Agents will be required to verify addresses by secondary means, most likely through field operations to interview neighbors, friends, and relatives to obtain information. Some of the information contained in DMV databases may be available from other sources, but this data is not as accurate, current, or complete as in the DMV databases. With the expenditure of additional time and effort, some DMV information may be located in other databases, but some records are specific to DMV databases. For example, commercially available public databases, such as CP CLEAR, contain some residential records, dates of birth, and photographs; however, this information is often incomplete, incorrect, or outdated. Some of the required information may be found in law enforcement databases as well, but this data is often outdated or incomplete. Direct access to DMV databases is required to ensure that the most accurate and current information can be obtained in a timely manner by ICE HSI when conducting operations or investigations.



- b. ERO: ICE ERO currently does not have an alternative way to obtain DMV or other listed database information when the responsible state or local administrators are barred by state law from providing access.
- c. OPR: There are no alternative ways to obtain this information as readily and accurately as via the DMV.

6. What are the short-term and long-term solutions available to address the security consequences if any, that result from losing access to DMV information?

- a. HSI: Without the ability to obtain DMV information independently and expeditiously, ICE HSI investigations and operations will suffer serious security consequences.

[REDACTED]

[REDACTED]

- b. ERO: There are no other resources that can replace the DMV data. In the short and long term, ICE ERO will work with less-reliable alternatives that remain available to continue its priority field investigations.
- c. OPR: There are no other resources available that could provide the same information as quickly and reliably as the DMV accessible information.

[REDACTED]

To: PLCY EXEC SEC[PlcyExecSec@hq.dhs.gov]
Cc: EXEC, USCG SMB[USCG.EXEC@uscg.mil]
From: EXEC, USCG SMB
Sent: Thur 1/9/2020 3:42:45 PM (UTC-05:00)
Subject: FW: AS1 memo to Operational Components (Service 1190329) (Intranet Quorum IMA007321014)

Good Afternoon PLCY,

As requested in the WF tasking, USCG sends response directly.

USCG CoS Captain Mark Fedor clears the below response to the subject tasking.

1. What DMV information is currently available to your Component and how is it accessed? None
2. How is DMV information used in the day-to-day operations of your Component? DMV information is not used
3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited? None
4. What are the long-term operational impacts of not having access to DMV information? None
5. Are there alternative ways to obtain the information contained in the DMV databases? None needed
6. What are the short-term and long-term solutions available to address the security consequences, if any, that result from losing access to DMV information? None needed

Thank you and have a wonderful day.

Very Respectfully,

Ms. Seville L. Henney, YN1
Executive Secretariat (ExecSec)
Office of the Commandant
United States Coast Guard
uscgexecsec@uscg.mil
PH: (202) 372-4538

-----Original Message-----

From: JOLLY BITTICK <IQ@IQ.DHS.GOV>
Sent: Monday, December 30, 2019 12:54 PM
To: EXEC, USCG SMB <USCG.EXEC@uscg.mil>
Subject: AS1 memo to Operational Components (Service 1190329) (Intranet Quorum IMA007321014)

Good morning CBP, CISA, FEMA, ICE, TSA, USCG, USCIS, USSS:

Please see Attachment #1, AS1's instructions regarding Operational Assessment of State Laws Restricting the Sharing of Department of Motor Vehicle Information with DHS.

Please confirm receipt of the memo by providing info copy to ESEC Internal and ensure coordination with PLCY to provide requested materials by the date requested (see Operational Assessment section).

For your convenience, PLCY has also been included on this info copy.

Thank you.

Contact: The Honorable Chad Wolf

https://urldefense.proofpoint.com/v2/url?u=https-3A_IQ.dhs.gov_iq_UX_serviceitem.aspx-3Fid-3D1190329-26IAccount-3DIQ&d=DwlFAg&c=0NKfg44GVknAU-XkWXjNqQ&r=wxn7qapRd4g9ApZYZRn8B4IBESfjbMPeZ7-yS_JBa4&m=YLFALgEnMwk5H4V-Mk3tIC6dR8JUyRDburFpSk3Ttx8&s=xiwSmaZiJKON72jiv09pZBxLcY2adjgTt1upPL0rhyA&e=



January 14, 2020

TO: Office of Strategy, Policy, and Plans
Department of Homeland Security

FROM: Immigration Records and Identity Services
U.S. Citizenship and Immigration Services

SUBJECT: Operational Assessment of State Laws Restricting the Sharing of Department of Motor Vehicle Information with DHS

This memo is in response to U.S. Citizenship and Immigration Services Operational Assessment of the subject matter above.

While there is no severe impact to USCIS operations and the E-Verify Program as a result of New Jersey and New York revoking access to driver's license data, there are identity management concerns with their recent actions. Immediately after the E-Verify Program began accessing and validating driver's license data through the National Law Enforcement Telecommunications System (NLETS), both states implemented technical solutions to prevent E-Verify access to the data. Unfortunately, E-Verify participating employers will have to rely on a physical inspection of driver's licenses from these states and make a subjective decision as to the validity of the document. This check of driver's license validity is less secure than validating data with the source Department of Motor Vehicle (DMV) database. NY/NJ are among the 9 states that do not currently allow E-Verify access to driver's license data. No state currently allows E-Verify access to driver's license photographs for verification purposes.

1. What DMV information is currently available to your Component and how is it accessed?
Components should identify each state and territory that currently restricts access to DMV information.
 - a. E-Verify currently accesses DMV data from 41 states plus DC and Puerto Rico through NLETS. There are 9 states (NY/NJ/CA/WA/VT/MD/NE/PA/ME) that do not allow access to DMV data for E-Verify purposes, and VA may soon cut off access.
2. How is DMV information used in the day-to-day operations of your Component?
 - a. E-Verify currently validates driver's license data supplied by recently hired employees against source data in DMV systems to validate the authenticity of the document used to confirm employees' identities.

3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?
 - a. E-Verify participating employers will have to rely on a physical inspection of driver's licenses from these states and make a subjective decision as to the validity of the document. This check of driver's license validity is less secure than validating data with the source DMV database, because the employer would not be able to confirm the DMV data and would rely on their own inspection. As employers are not document inspection experts, this would be less secure.
4. What are the long-term operational impacts of not having access to DMV information?
 - a. While there are no operational impacts to USCIS or E-Verify, E-Verify participating employers will have to rely on a physical inspection of driver's licenses from these states and make a subjective decision as to the validity of the document. This check of driver's license validity is less secure than validating data with the source DMV database. Therefore, E-Verify would not work as well as it could if access to DMV information is limited.
5. Are there alternative ways to obtain the information contained in the DMV databases?
 - a. We are currently unaware of any other services that give access to DL data from the states that are preventing access. We continue to work with those states who have refused access and encourage them to work with the Department on this unique identity management and security enhancement initiative.
6. What are the short-term and long-term solutions available to address the security consequences, if any, that result from losing access to DMV information?
 - a. We continue to reach out to the DMVs who have prevented access to their DL dataset for E-Verify purposes and will explore any other solutions that DMVs propose so that E-Verify can access their dataset.

U. S. Secret Service Response

1. What DMV information is currently available to your Component and how is it accessed? Components should identify each state and territory that currently restricts access to DMV information.

Driver's license and vehicle registration information is available from participating states through Nlets and is accessed by the United States Secret Service (USSS) via the eAgent application.

Driver's License

Positive driver's license responses may contain the driver's name, address, date of birth, physical description, Social Security number, license type, restrictions, status, and license number. A driver's license response may include an image if one was requested and is available. Driver history information can also be obtained.

A driver's license can be queried using the license number. Some states support inquiry by name and date of birth.

States that do not respond to inquiries by name only include AL, AZ, CA, CO, FL, GA, HI, IA, IL, IN, MA, MI, MN, MO, MS, NB, ND, NH, NJ, NM, NY, OH, OR, PR, RI, UT, VA, VI, VT, WA, WI and WY.

All states participate in driver history sharing except IL, PR and VI.

All states participate in driver's license photo sharing except AK, CA, CO, CT, DC, HI, IL, KS, ND, NH, NV, NY, OK, PR, SC, VI and VT.

Vehicle Registration

Positive vehicle registration responses may contain information including the registered owner, license number, license type, license year, VIN, vehicle model, vehicle style, and vehicle color.

A vehicle registration can be queried using the vehicle identification number (VIN) or license plate/license year/license type. Some states support inquiry by name and date of birth.

States that do not respond to inquiries by name only include AK, AL, AR, AZ, CA, CO, FL, GA, HI, IA, IL, IN, MA, MD, MI, MN, MO, NB, ND, NH, NJ, NM, NY, OH, OR, PA, PR, RI, TN, TX, UT, VA, VI, VT, WA and WI.

2. How is DMV information used in the day-to-day operations of your Component?

Information obtained from DMV helps USSS quickly verify the identity of suspects through the personal information and description provided in the response. The address listed will also help us determine a possible location. The availability of photos also helps confirm the identity of a person.

3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?

Accessibility of DMV information to the law enforcement community should be given high priority.

4. What are the long-term operational impacts of not having access to DMV information?

Information-sharing among law enforcement agencies and entities charged with public safety is vital in the prevention of crimes.

5. Are there alternative ways to obtain the information contained in the DMV databases?

There are commercial databases (*i.e.*, Accurint, Clear, LexisNexis, Courtlink, TLO, etc.) that can be utilized to search for addresses, personal information, assets and court documents that can aid us in our investigations. The information obtained from these databases, however, may not be as current as the driver's license information obtained from DMV.

6. What are the short-term and long-term solutions available to address the security consequences, if any, that result from losing access to DMV information?

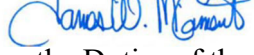


Homeland
Security

January 27, 2020

INFORMATION

MEMORANDUM FOR THE ACTING SECRETARY

FROM: James W. McCament 
Senior Official Performing the Duties of the Under Secretary
Office of Strategy, Policy, and Plans

SUBJECT: Component Operational Impact Assessments of State Laws Restricting the
Sharing of DMV Data with DHS

Purpose: To provide an assessment of the impact of state laws restricting Department of Homeland Security (DHS) access to state Department of Motor Vehicle (DMV) information.

Consolidated Assessment: In your December 30, 2019 memorandum, you directed DHS operational Components to answer six questions regarding their access to DMV data and the resulting impacts to mission operations if states restricted that access. U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) indicated that restricting access to DMV information would significantly impact their operations. U.S. Secret Service (USSS), Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), U.S. Citizenship and Immigration Services (USCIS), and United States Coast Guard (USCG) all reported either no or uncertain impacts at this time.

1. What DMV information is currently available and how is it accessed?

DMV records include information about registered vehicles and individuals who have been issued driver's licenses. Vehicle information may include vehicle identification number, current and prior license plate number(s), vehicle make/model/year/color, vehicle type, lienholder information, and the name and address of current and prior registered owner(s). Driver's license information may include the license holder's name, address, photograph, license status, height and weight, hair and eye color, gender, license number, social security number, and date of issuance/expiration.

Generally, DHS Components are able to access DMV information through the National Law Enforcement Telecommunication System (Nlets), which is available for CBP and ICE Enforcement and Removal Operations (ERO) through its TECS system and for ICE Homeland Security Investigations (HSI) through its Investigative Case Management (ICM) system. In addition to access through Nlets, some states provide DHS law enforcement Components direct access to their DMV databases, and some states direct ICE to obtain data through their local

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 2

fusion centers, through state and local partners, or through court orders. The amount of DMV information available to ICE varies from state to state.

New York's Law Restricting DHS's Access to Its DMV Information: New York recently implemented a law blocking ICE and CBP from accessing its DMV information.¹ It also threatened to block access to other state law enforcement agencies and departments if they provide New York DMV records to ICE and/or CBP. A limited number of ICE HSI New York agents have access to NY DMV data through an e-portal system called E-justice. However, this is only available to HSI NY agents and does not alleviate the access issues for the remainder of ICE or CBP.

Other States and Territories Restricting DMV Information Access to DHS:



2. How is DMV information used in the day-to-day operations of your Component?

ICE

ICE HSI: HSI uses DMV information daily to identify, locate, and associate individuals and vehicles as part of ongoing investigations covering the full range of HSI investigative categories including, but not limited to: narcotics smuggling, child exploitation, human smuggling and trafficking, trans-national gangs, national security, identity and benefit fraud, financial, and intellectual property rights. DMV information is often used to verify or corroborate demographic information associated with an individual. DMV information can be factual evidence used in affidavits as supporting evidence for residency needed to acquire a judge's

¹ New York's recently implemented "Green Light Law" prohibits its DMV commissioner from disclosing DMV information "to any agency that primarily enforces immigration law" without a court order or warrant. It also requires anyone else who receives access to New York DMV information to certify that they will not use the information for civil immigration purposes or disclose the information to any agency that primarily enforces immigration law. The New York law defines "agency that primarily enforces immigration law" to include ICE and CBP. If an immigration agency requests DMV information, the New York law requires its commissioner to notify the individual about whom such information was requested, within three days that the request was made and the identity of the agency that made the request.

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 3

signature on federal search warrant applications. It is also critical for building out criminal networks and creating new leads for investigation.

DMV photograph information is used to compile photographic line-ups to be used in the field or during interviews and while conducting facial recognition searches to identify individuals or targets. Further, access to license plate information assists ICE with tracking vehicles through both use of automated license plate reader technology and physical surveillance.

The ability to retrieve vehicle and driver's license/identification information in near real-time assists in identifying possible targets, witnesses, victims, and assets, and deconflicting with other local, state, and federal law enforcement agencies. DMV information also is crucial to officer safety including during the execution of an arrest or search warrant, where such information assists in identifying individuals who might pose a threat based on criminal history or other factors.

ICE ERO: ERO uses state DMV information to query driver license history/issuance, vehicle registration history/issuance, incident/accident reports, and cross reference for other investigative leads during encounters of suspected foreign-born nationals. ERO's Targeting Operations Division (TOD) uses driver's license/DMV searches in varying ways to establish targetability, confirm identity and residence, and determine other relevant information, such as a subject's last known location. This is used to develop target packages used by the 24 field offices to identify, and locate removable aliens, including criminal aliens in the interior United States.

ERO officers would also use this information to review and verify a subject's identity against DHS indices. The loss of the ability to corroborate a subject's identity (or identities) using driver's license information compromises officer safety while enabling persons to evade detection with false or fraudulent ID information.

Office of Professional Responsibility (OPR): OPR investigates criminal violations across the full spectrum of the federal code, including allegations of public corruption. OPR routinely uses DMV information and/or photos while conducting criminal investigations to identify and locate suspects, witnesses, victims of crime, and assets that may be subject to seizure. Restricting access to DMV information significantly impacts OPR's ability to protect the homeland and enforce federal criminal laws.

Additionally, from a personnel security standpoint, while conducting criminal inquiries on ICE applicants, OPR obtains Nlets and DMV information. The DMV information is used to determine if an inordinate number of traffic violations have occurred within given timeframes, as many of ICE's law enforcement positions require the operation of a government-owned vehicle on a routine basis. OPR also obtains TECS hits involving suspected drug smuggling operations that may be related to an ICE applicant. These TECS hits usually contain vehicle information, and OPR uses the vehicle information to conduct vehicle registration inquiries through the appropriate state to ascertain if the registered vehicle correlates to the applicant in question.

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 4

CBP

Trusted Traveler Programs (TTP): Approximately 9.5 million travelers are currently enrolled in CBP's four TTPs. These programs expedite the processing of known, low risk, vetted travelers arriving into and departing from the United States, permitting CBP officers additional time to focus on higher risk, unknown travelers. Another TTP program, the Free and Secure Trade (FAST) Program (containing 76K members), is a commercial clearance program for known low-risk commercial shipments entering the United States from Canada and Mexico. Identity confirmation is a critical element in establishing eligibility to participate in any of CBP's TTPs. Access to DMV information through Nlets helps CBP in confirming identity and making eligibility determinations for issuance of its TTP cards which can serve in lieu of a passport at land borders. More than [REDACTED] NY residents are CBP TTP members and over [REDACTED] NY residents have a TTP application pending vetting. In calendar year 2019, NY state residents who are TTP members have entered the United States via the northern land border more than [REDACTED] times and arrived via air into the NY state area more than [REDACTED] times. In 2019, a total of [REDACTED] NY licensed drivers utilized FAST lanes to cross the northern land border a total of [REDACTED] times.

Enhanced Driver's License (EDL) Program: EDLs are essentially a way to allow U.S. citizens to use their driver's licenses in place of a passport for international travel into Canada. They are based on an agreement between U.S. states and DHS. DHS allows states to issue documents that can serve for land or sea border crossings as long as they meet certain security requirements and that the states share their EDL data with DHS, so that DHS can quickly validate the legitimacy of the documents when the bearer crosses the border. New York state residents are not required to get an EDL to obtain a driver's license. The plain language of the Green Light law would violate the 2007 Memorandum of Agreement (MOA) that New York already has with DHS, and that is the agreement on which all EDLs issued in New York is based.

State-issued EDLs provide proof of identity and U.S. citizenship, are issued in a secure process, and include technology that makes travel easier. They provide travelers with a low-cost, convenient alternative for entering the United States from Canada, Mexico, or the Caribbean through a land or sea port of entry, in addition to serving as a permit to drive. Currently, five states (Michigan, Minnesota, New York, Vermont and Washington) issue EDLs through MOA with DHS that allows CBP to validate a traveler's identity and citizenship at time of issuance and upon each presentation at a border crossing. The MOA provides that either party may terminate the MOA by providing written notice thirty (30) calendar days in advance of the termination. While NY has not notified CBP of an intention to terminate the MOA, there is a strong likelihood that NY will withdraw from the MOA in light of the Green Light Law. Preventing CBP from accessing driver's license and registration data stored in TECS and validating means it can no longer validate a traveler's identity with the EDL. Given that New York has issued approximately 2.3 million EDLs, shutting down the program would have a significant operational impact. The highest three volume locations for NY EDLs [REDACTED] saw up to [REDACTED] NY EDL crossings in August 2019, which was the busiest month being with more than [REDACTED] crossings daily in these locations alone.

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 5

Vehicle Exports: CBP must determine eligibility of vehicles titled in NY, specifically to verify clear ownership of the vehicle by the exporter. Retrieval of registration and lien data is performed at inspection in accordance with 19 C.F.R. §192.2 which requires the advance submission and authentication by CBP of both the vehicle and supporting documentation, in this case a U.S. issued certificate of title. CBP estimates that there were approximately 42,000 vehicles exported in 2019 with NY titles. Without access to NY DMV NLETS data CBP is required to manually authenticate the vehicle and supporting data. Manual verification would require a physical inspection for each vehicle. Assuming a minimum of 1 hour per additional inspection, conducted by 2 CBPOs, that would be approximately 84,000 additional hours of labor or 40 FTE

3. What are the security consequences, if any, to your day-to-day operations if DMV information is unavailable or limited?

ICE

HSI: If DMV information were not made available to HSI for use in its investigations, it would be extremely difficult to quickly identify criminal suspects and unnecessarily prolong investigations potentially putting victims, the general public and agents at risk. This is especially crucial in crimes involving child exploitation and human trafficking. Additionally, the inability to quickly access an individual's criminal history, warrant status, or an armed/dangerous alert could unnecessarily endanger agents in the field. Limiting or eliminating access to DMV information could also increase incidents of interfering with other ongoing local, state, and federal criminal investigations. Numerous state DMVs maintain firearms registration information. The loss of access to firearms registry information also presents a serious impediment to officer safety.

For example, several high-profile acts of domestic terror have recently occurred in the New Jersey/New York area. Access to New Jersey and New York DMV information is imperative to ensure officer and public safety.

- On December 10, 2019, over several hours, two individuals killed a Jersey City, New Jersey Police Officer and three other people in Jersey City, New Jersey, and shot at law enforcement, including ICE HSI personnel. Inside their rented U-Haul were two pipe bombs. One of the subjects also owned another vehicle that was not immediately located. ICE HSI Newark personnel on-site attempted to query New York DMV for this license plate but were restricted from accessing it.
- On December 19, 2019, the New York State Office of General Counsel (NYSOGC) contacted ICE HSI Newark regarding a New York DMV system query that was run out of the ICE HSI Newark Field Office. NYSOGC informed ICE HSI Newark that, pursuant to recently-enacted legislation, all access by ICE, CBP, and USCIS was terminated. In addition, within 3 days of the query, NYSOGC was bound by the new law to notify the individual that ICE attempted to access their information.
- On December 28, 2019, an individual in Monsey, New York, entered a synagogue, stabbed five congregants, critically injuring one, and then fled. A witness provided

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 6

license plate information which was then disseminated to the New Jersey/New York law enforcement community. ICE HSI personnel attempted to query the license plate information but were unable to due to state restrictions. ICE HSI personnel requested that an ICE HSI Task Force officer obtain the information and the information was returned in one and a half hours. The subject was eventually stopped in New York City with the assistance of license plate recognition technology.

ERO: ERO investigations and operations are impeded if the case relied upon these database leads to establish probable cause. The TOD's inability to return DMV data will have a direct impact to officer safety, as the division will be unable to corroborate identity using driver's license information. This could enable persons to fraudulently use other identities to evade detection. In addition, decreased information and data-sharing between state and local DMV entities and the TOD would produce the following impacts:

- lost access to standard driver license, vehicle queries, and criminal history specific to the state;
- inability to access DMV information to assist with at-large sex offender investigations;
- inability to access DMV information to assist with at-large aggravated felon investigations;
- inability to access DMV information to assist with at-large Egregious Public Safety (EPS) investigations referred by USCIS;
- inability to access DMV information to assist with at-large Interpol fugitive investigations; and
- inability to access DMV information to assist with at-large criminal alien investigations.

OPR: Limiting or providing no access to critical information, such as a subject's photograph, last known address, physical attributes, and vehicle registration information, can pose serious officer safety risks to law enforcement officers engaging in operational activities. Time-sensitive circumstances require direct and immediate access to DMV data to mitigate potential life-threatening situations.

Additionally, without the ability to obtain state DMV information, ICE risks having personnel security make favorable suitability and national security determinations on applicants who have suspended/revoked drivers licenses. Furthermore, without the ability to verify vehicle registration information, ICE would be restricted in obtaining valuable information that is critical in making sound suitability and national security determinations.

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 7

4. What are the long-term operational impacts of not having access to DMV information?

ICE

HSI: Long-term loss of DMV information would severely impede ICE HSI's ability to identify, locate, and arrest individuals violating federal law and severely hinder its ability to investigate, disrupt, and dismantle transnational criminal organizations in every case category. This would result in fewer arrests, wasted resources, and a diminished number of otherwise successfully resolved investigations. [REDACTED]

[REDACTED] The absence of readily available and reliable DMV information will increase the risk of prematurely exposing sensitive investigations due to the necessity of using alternate methods to identify the identical information contained in DMV records.

ICE HSI agents also rely upon DMV information in affidavits for federal and state search and arrest warrants. These warrants require that the agent identify the place and person to be searched or arrested. This is accomplished by running driver's and vehicle information and cited as such in the affidavits. Matching individuals or their car to their driver's license is a commonly accepted law enforcement method of identifying an individual. Additionally, DMV information allows the agent to determine if the individual is the subject of an outstanding arrest warrant (to include those issued by state and county agencies). Without this information, agents may encounter wanted criminals and release them.

ERO: ERO identification, arrest, detention, and removal of foreign born nationals, including those who are high-priority for removal, will be negatively impacted. The TOD will lose a large amount of data that is currently used to determine the current and last known addresses of criminal aliens, including egregious offenders, gang members, national security threats, and recidivist criminals. Absent this information, the TOD will be unable to build target packages for the field, significantly limiting the number of interior arrests ICE ERO will be able to make on an annual basis. This will result in negative effects on public safety and national security.

OPR: The long-term impact of not having access to DMV information would result in inefficiencies or delays in identifying and locating targets and victims of criminal investigations, as well as law enforcement operations and surveillance during ICE OPR investigations. Furthermore, any restriction in obtaining DMV or NLETS information would have immense consequences in ICE making sound suitability and national-security determinations on its job applicants. These restrictions would continue to compound the longer the restrictions were in place, which would result in ICE employing numerous applicants who would have otherwise been found ineligible for employment.

Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 8

5. Are there alternative ways to obtain the information contained in the DMV databases?

ICE

HSI: Agents will be required to verify addresses by secondary means, most likely through field operations to interview neighbors, friends, and relatives to obtain information. Some of the information contained in DMV databases may be available from other sources, but this data is not as accurate, current, or complete as in the DMV databases. With the expenditure of additional time and effort, some DMV information may be located in other databases, but some records are specific to DMV databases. For example, commercially available public databases, such as CP CLEAR, contain some residential records, dates of birth, and photographs; however, this information is often incomplete, incorrect, or outdated. Some of the required information may be found in law enforcement databases as well, but this data is often outdated or incomplete. Direct access to DMV databases is required to ensure that the most accurate and current information can be obtained in a timely manner by ICE HSI when conducting operations or investigations.

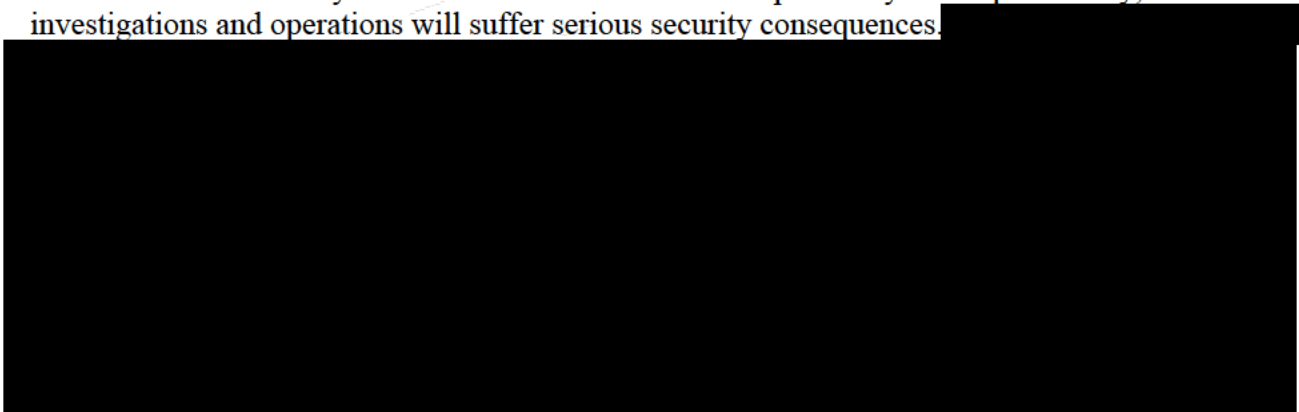
ERO: ERO currently does not have an alternative way to obtain DMV or other listed database information when the responsible state or local administrators are barred by state law from providing access.

OPR: There are no alternative ways to obtain this information as readily and accurately as via the DMV.

6. What are the short-term and long-term solutions available to address the security consequences if any, that result from losing access to DMV information?

ICE

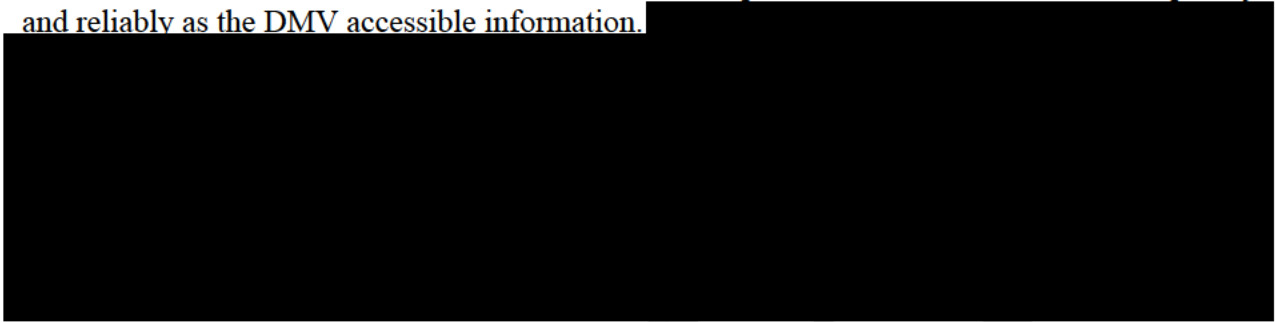
HSI: Without the ability to obtain DMV information independently and expeditiously, ICE HSI investigations and operations will suffer serious security consequences.



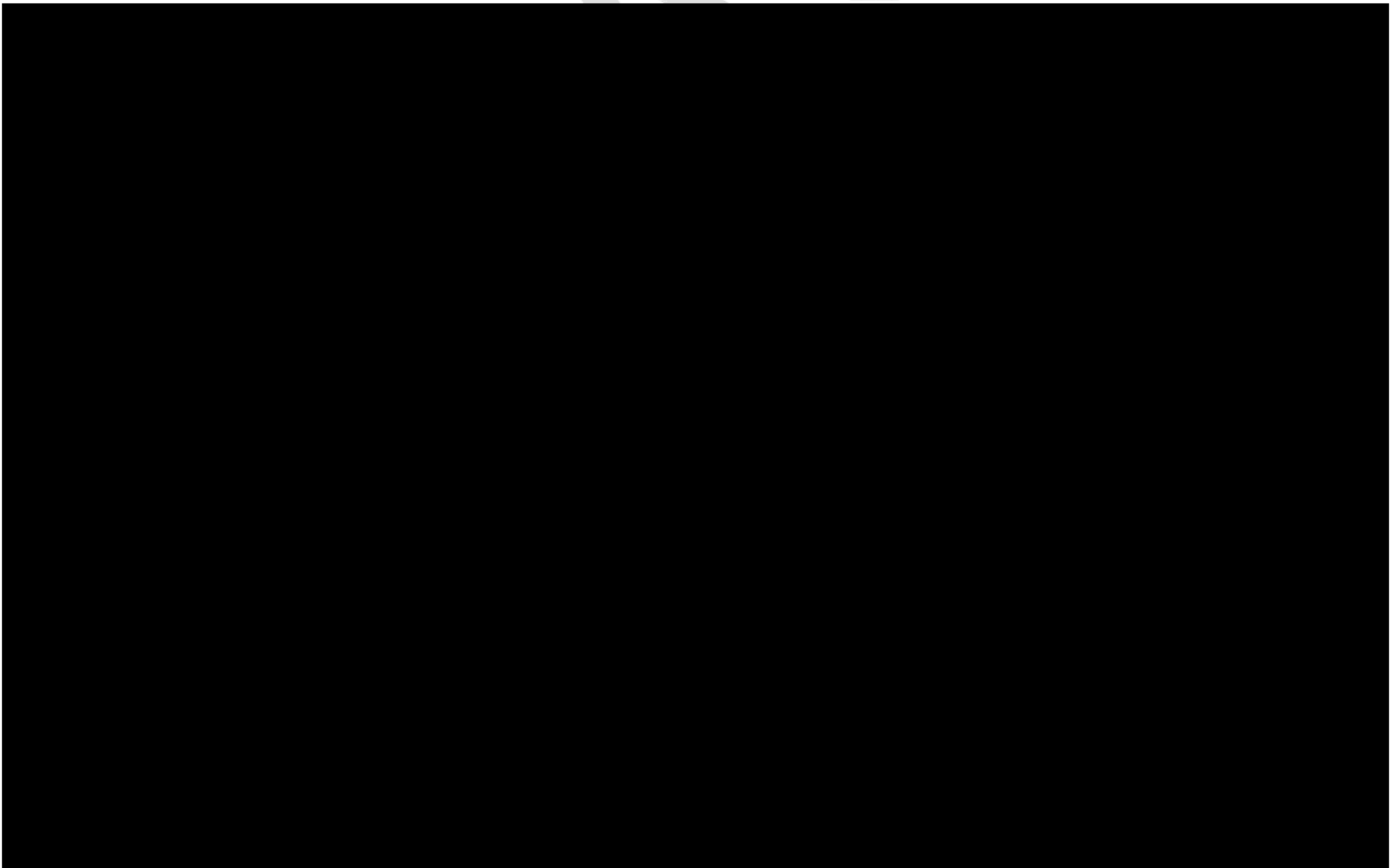
Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 9

ERO: There are no other resources that can replace the DMV data. In the short and long term, ICE ERO will work with less-reliable alternatives that remain available to continue its field investigations. However, it is important to understand that this limitation will profoundly impact, in an adverse way, ERO's ability to locate and arrest aliens unlawfully present in the relevant area of responsibility.

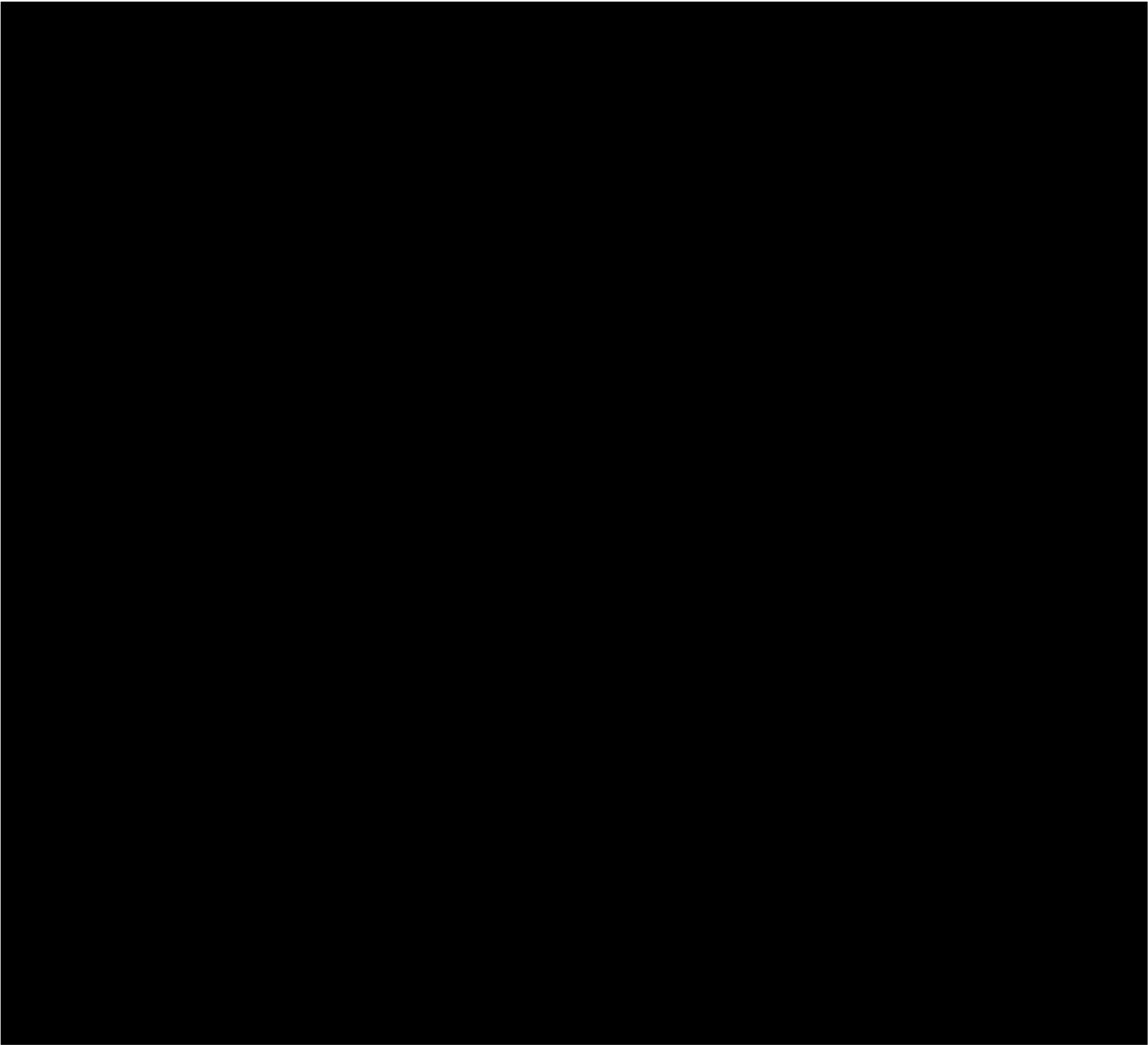
OPR: There are no other resources available that could provide the same information as quickly and reliably as the DMV accessible information.



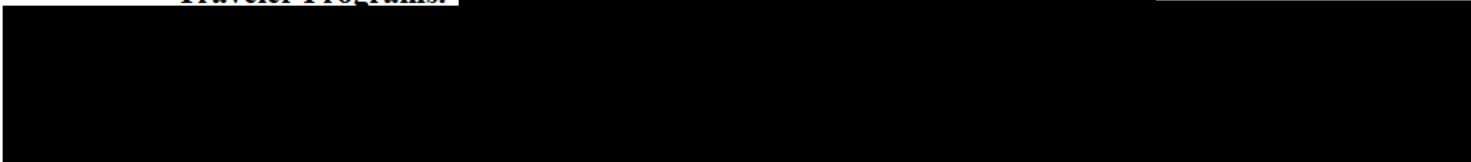
Options for addressing laws that restrict access to state DMV information: Upon review of Component responses, PLCY is presenting options to consider in response to the impact of the NY Green Light Law and other laws restricting access to state DMV information.



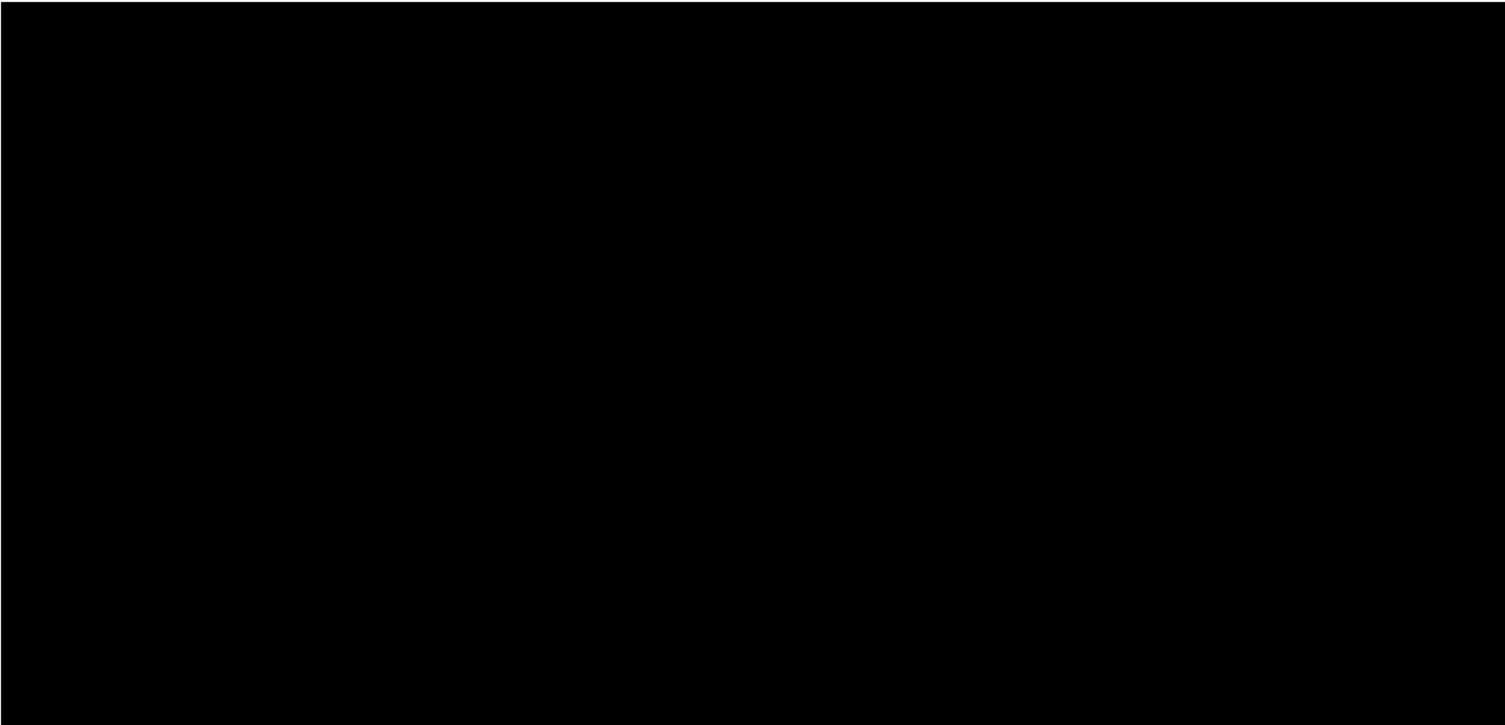
Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 10



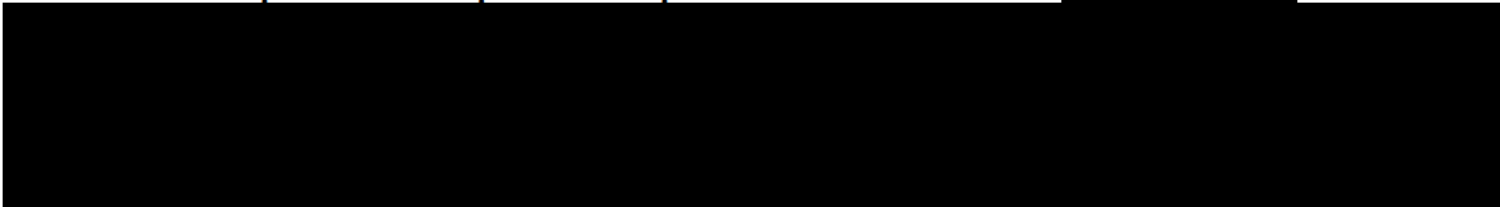
- 5. Exclude residents of uncooperative states from participating in DHS Trusted Traveler Programs.**



Subject: Assessments of State Laws Restricting the Sharing of DMV Data with DHS
Page 11



8. De-prioritize the export of uncooperative state-titled vehicles.





**Memorandum of Agreement
Between the
New York State Department of Motor Vehicles
And the
United States Department of Homeland Security**

I. PARTIES

The Parties to this Memorandum of Agreement (hereinafter "MOA") are the Department of Homeland Security, hereinafter referred to as "DHS," and the New York State Department of Motor Vehicles, hereinafter referred to as "DMV" (collectively, the "Parties").

II. AUTHORITY

DHS is authorized to enter into this MOA pursuant to the Homeland Security Act of 2002, 6 U.S.C. § 112(b), as amended. DMV is authorized to enter into this MOA pursuant to New York State Vehicle & Traffic Law §§ 200, 494 and 508.

III. ENHANCED DRIVER LICENSE

A. PURPOSE

This MOA demonstrates the Parties' shared commitment to voluntarily offer in New York State an enhanced driver license and enhanced non-driver identification card. (The documents issued by New York State as an enhanced driver license or non-driver identification card will be collectively referred to in this MOA as the "Enhanced Driver License"). Under the voluntary project, DHS and DMV will develop and issue an Enhanced Driver License with facilitative technology to be used for border crossing purposes. The Secretary of Homeland Security expects to propose that a valid and lawfully obtained enhanced New York State driver license, or identification card for those who do not drive, be accepted as an alternative Western Hemisphere Travel Initiative (WHTI) document for land and sea border crossings. The project will allow the Parties to assess the desirability of offering the Enhanced Driver License as acceptable documents for WHTI. The Secretary of Homeland Security also expects the enhanced driver's license to align with Real ID requirements, generally consistent with the phases to be outlined in the Real ID final rulemaking.

B. BACKGROUND

WHTI implements a Congressional requirement that all United States citizens and other travelers to and from Canada, Mexico, Central and South America, the Caribbean and Bermuda present a passport or other accepted document that denotes the bearer's identity and citizenship to enter or re-enter the United States. The goal is to strengthen border security and facilitate entry into the United States for U.S. citizens. It is anticipated that the date of full WHTI implementation will

be in the summer of 2008. At that time, U.S. citizens traveling between the U.S. and Canada, Mexico, Central and South America, the Caribbean, and Bermuda by land or sea (including via ferries), may be required to present a valid U.S. passport or other document acceptable to the Secretary of Homeland Security.

The Parties anticipate that a New York State Enhanced Driver License will be an acceptable alternative document for U.S. citizens. Such an enhanced New York State document would advance the economic interests of Upstate New York, the State of New York and DHS.

The driver license is a nationally accepted means of identification. It is recognized that New York State already has strong procedures to securely confirm identity, and has recently increased that security through a number of anti-fraud security measures. New York's driver license and non-driver identification card can be enhanced to denote citizenship, based upon DMV's legislatively-granted power to establish internal procedures prescribing the manner in which licenses and non-driver identification cards are issued and what information must be submitted to obtain those documents. The holder of the New York State Enhanced Driver License will be able to use such a document to drive or to identify him or herself as well as denote citizenship at a border crossing – at a cost and convenience savings to the applicant.

New York residents enjoy traveling, shopping and vacationing in Canada. Similarly, Canadian residents enjoy traveling, shopping and vacationing in New York, greatly contributing to New York's economy. Recognizing that a significant portion of trade between the United States and Canada occurs at New York's multiple border crossing between the Provinces of Ontario and Quebec, a successful project of the Enhanced Driver License would greatly assist in continuing tourism and trade with Canada. This will increase the overall efficiency of the border crossing process, thereby reducing wait times for all.

A successful project will also serve the interests of DHS by increasing the use of facilitative technology, thereby facilitating cross border trade and travel, and providing an enhanced state driver license or identification card that can meet the security goals of the Congressional mandate.

C. PROJECT RESPONSIBILITIES

DMV shall be responsible for:

- (1) Issuing an Enhanced Driver License which denotes, pursuant to issuance standards jointly agreed upon by the Parties and provided for in a business plan to be developed by DMV, the identity and U.S. citizenship of New York State residents.
- (2) Including facilitative technology in or associated with the use of an Enhanced Driver License, that has been agreed to by DHS, to facilitate identity and citizenship validation through the sharing of information and include the current status of the card holder's right to use the Enhanced Driver License for cross border travel purposes.

(3) Developing a business plan for the voluntary project, in conjunction with DHS, which implements minimum business requirements acceptable to DHS, including incorporating Real ID requirements and protecting personally identifiable information.

(4) Providing DHS with the opportunity to review the operations of the project and responding to any Enhanced Driver License-related comments from DHS.

(5) Ensuring that employees involved in the project have undergone background checks as mutually agreed upon by the Parties.

The Department of Homeland Security shall be responsible for:

(1) Accepting, for purposes of WHTI, pending publication of regulations/notice on acceptable documents, New York State's denotation of identity and citizenship associated with an Enhanced Driver License that New York State issues.

(2) Providing facilitative technology specifications for the Enhanced Driver License, providing the facilitative technical specifications for an interactive validation process and utilizing these facilitative technologies.

(3) Establishing minimum standards for the project including issuance standards for the Enhanced Driver License.

(4) Approving a detailed New York State business plan for the project which implements minimum business standards mutually agreed to with New York State.

(5) Reviewing the operation of the project pursuant to the business plan and providing comments to New York State.

(6) Protecting the information shared and limiting its use to the intended purposes of this project.

It is intended that both the DMV and DHS will work in good faith to accomplish the preceding responsibilities in a timely manner so that implementation of the project will be accomplished approximately concurrent with the implementation of the requirement that individuals have a passport or other acceptable document to cross the land and sea borders consistent with the WHTI final rule.

D. POINTS OF CONTACT

FOR DHS:

Colleen M. Manaher
Director, WHTI PMO

FOR DMV:

Wayne L. Benjamin,
Executive Deputy Commissioner, New York State Department of Motor Vehicles

IV. DRIVER LICENSE SECURITY

DMV shall be responsible for:

- (1) Adopting procedures as soon as operationally practicable to issue Real ID compliant driver licenses and identification documents for non-U.S. citizens that identify the expiration of the legal presence document presented by the non-U.S. citizen, and institute processes to issue licenses that expire co-terminus with the legal presence document, and ensuring that the document's expiration date in no case exceeds 8 years from issuance.
- (2) Consistent with the requirements of the Real ID Act, clearly marking driver licenses and identification documents as not acceptable for official U.S. Government purposes, as that term is defined under the Real ID final rule once published, that are issued to individuals who have not established legal presence in the United States, and proceeding in a way that no licenses or identification documents shall be issued to such individuals until this marking provision is implemented.
- (3) Instituting a residency requirement for the issuance of New York driver license or identification cards before issuing such documents to individuals who have not established legal presence in the United States.
- (4) Taking steps to become Real ID compliant as soon as operationally practicable after the Real ID final rulemaking is published.

V. TERM AND TERMINATION

Either Party may terminate this MOA upon the giving of written notice thirty (30) calendar days in advance of the termination date to the other Party.

VI. MODIFICATION

Modifications within the scope of the MOA shall be made by mutual consent of the Parties, by the issuance of a written modification, signed and dated by both Parties.

VII. EFFECTIVE DATE

This MOA is effective on the date of the last signature hereon by the Parties.

VIII. CONFIDENTIALITY

Each Party understands that the other Party or third parties may disclose to it information designated by another party as confidential information related to the project discussed in this MOA ("Confidential Information").

Each Party agrees to maintain in confidence such information and will use this information solely to provide services related to the project under this MOA. Except as required by law, each Party shall not disclose this information to any person except authorized contractors who also agree not to disclose this Confidential Information. Each Party shall include requirements of

confidentiality for any person that has access to the Confidential Information pursuant to this MOA.

Each Party shall take reasonable measures to maintain the confidentiality of this information pursuant to the business plan. Each Party will immediately give notice to the other Party of any request for, use of or disclosure of Confidential Information and agrees to assist the other in responding to any request, remedying any use, or remedying any disclosure.

Further, DHS agrees that all materials containing Confidential Information received pursuant to this MOA concerning New York State's residents and its employees, and any other information which may be classified as confidential, shall not be disclosed to other persons without New York State's written consent except as may be required by law. Any personal information received by DHS shall be handled by DHS, as appropriate and necessary, in accordance with the Privacy Act of 1974, as amended.

Notwithstanding any other provision of this Agreement, disclosure of Confidential Information shall not be precluded if such disclosure is in response to a valid order of a court order or other governmental body or is otherwise required by law; provided, however, that the party responding to the order or other legal requirements shall first give notice to the other party hereto and shall have, as appropriate:

- (a) fully cooperated in the other party's attempt to obtain a "protective order" from the appropriate court or other governmental body, or

- (b) attempted to classify such documents to prevent access by the public, in accordance with the provisions of the federal Freedom of Information Act ("FOIA") or similar State statutes.

IX. MISCELLANEOUS

This MOA does not confer a right or benefit on behalf of any third party and does not otherwise confer a right on any third party to enforce a term of this MOA.

This MOA represents the entire agreement between the Parties. No other understanding, oral or otherwise, regarding the subject matter of this MOA shall be deemed to exist or to bind any of the parties hereto.

This MOA does not obligate DHS funds for the State of New York Enhanced Driver License project.

This MOA may be executed in counterparts and/or via signatures transmitted by facsimile.

IN WITNESS WHEREOF, the Parties have signed two (2) duplicate originals of this MOA.

Department of Homeland Security

(Signature)

(Date)

10/27/07

Michael Chertoff

(Print Name)

State of New York

(Signature)

(Date)

10/27/07

Eliot Spitzer

(Print Name)

Secretary, Department of Homeland Security

(Title)

Governor, State of New York

(Title)

New York State Department of Motor Vehicles

(Signature)

(Date)

David Swarts

(Print Name)

Commissioner, NYS DMV

(Title)

Consolidated Trusted Traveler Programs Handbook

Revised April 2016

Foreword

This handbook establishes the policies and procedures for the Trusted Traveler Programs (TTP). These guidelines include the process for enrollment of travelers into the programs and the procedures for inspecting TTP members at the ports of entry. These programs are an essential element of the U.S. Customs and Border Protection (CBP) strategy to secure our borders through increased advanced knowledge of the travelers. TTP participants are subjected to rigorous vetting and random compliance checks to ensure the integrity of the programs. Shorter wait times and expedited procedures for Trusted Travelers at the ports of entry provide the incentive for participation in the programs.

The handbook provides an overview and guidance for CBP officers and supervisors who are assigned at the enrollment centers as well as those at the ports of entry. Officers and supervisors are advised to check the CBP website often for TTP updates, changes or additions to the policies and procedures outlined in this handbook. Frequent upgrades in technology, software, and issue resolutions result in recurrent procedural and/or policy changes.

**Assistant Commissioner
Field Operations**

1. Overview of the Trusted Traveler Programs

U.S. Customs and Border Protection (CBP) is committed to enhancing legitimate trade and travel while maintaining the highest level of border security and integrity. Trusted Traveler Programs (TTP) allow pre-enrolled, low-risk participants to receive expedited border processing, enabling CBP to direct additional scrutiny to the unknown, potentially higher risk, travelers arriving at ports of entry. The integrity of the TTPs is maintained by a strict screening process that includes: queries of multiple law enforcement databases and biometric validation of identity prior to enrollment; 24-hour checks to continually verify low risk status of enrolled travelers; and a system of randomized referrals to secondary inspection to ensure Trusted Traveler members are in compliance with all policies and regulations of TTP.

There are currently four TTPs: Secure Electronic Network for Travelers Rapid Inspection (SENTRI), NEXUS, Global Entry, and Free and Secure Trade (FAST). The four TTPs use a harmonized Global Enrollment System (GES) and on-line internet-based, Global Online Enrollment System (GOES). Upon submission through GOES, applications are forwarded to the Vetting Center (VC) where they undergo a strict vetting process. If no derogatory information is found, the application is conditionally approved by the VC. If derogatory information is discovered, the application may be denied. If the applicant passes the preliminary vetting process, he/she is asked to make an appointment at an Enrollment Center (EC) where CBP officers will confirm identity, review travel documents, verify admissibility status, complete 10-print fingerprint [REDACTED], and conduct an interview of the applicant. If the officer determines that the applicant is eligible for the program, he/she will be enrolled into the TTP for a five-year period.

1.1 SENTRI

SENTRI provides expedited CBP processing for pre-approved, low-risk travelers at southern land border ports of entry. At some locations, the SENTRI program is available for both vehicle and pedestrian border crossers. Each of the participating ports has designated SENTRI vehicle and/or pedestrian lanes with access restricted to SENTRI members. Participation in SENTRI requires that vehicles used to cross the border must be registered and inspected. Members are issued radio frequency identification (RFID) enabled SENTRI cards. The SENTRI identification document satisfies the Western Hemisphere Travel Initiative (WHTI) entry document requirements for citizens of the United States and Canada for land and sea travel. Access to the SENTRI vehicle lanes begins south of the border in Mexico, or on the access bridges, and is generally controlled by Mexican authorities. SENTRI members may use the NEXUS lanes when entering the U.S. from Canada. SENTRI members who are U.S. citizens or U.S. Lawful Permanent Residents may also use Global Entry kiosks.

1.2 NEXUS

NEXUS is a bi-national TTP operated jointly by the United States and Canada. NEXUS provides expedited CBP and Canada Border Services Agency (CBSA) processing for travelers entering both the U.S. and Canada via the air, land, or sea environments. Each applicant must be approved by both CBP and CBSA prior to enrollment. At land border locations, NEXUS lanes are available for entry into the United States as well as Canada. Members are issued RFID enabled NEXUS identification cards. The NEXUS identification card satisfies the WHTI entry document requirements for citizens of the United States and Canada for air, land and sea travel. All NEXUS members use Global Entry kiosks for expedited CBP processing at airports, to include U.S. preclearance locations in Canada. At Canadian airports, NEXUS members use NEXUS kiosks to enter Canada. The NEXUS kiosks use a biometric iris scan to verify program membership. NEXUS can also be utilized for small boat arrivals from Canada, providing for expedited processing. NEXUS members may use the SENTRI lanes at southern land border ports of entry, provided they travel in a SENTRI registered vehicle and comply with SENTRI requirements. NEXUS members can also use the SENTRI pedestrian lanes

1.3 Global Entry

Global Entry is the TTP at U.S. airports. Travelers enrolled in Global Entry utilize Global Entry kiosks in lieu of being processed by a CBP officer on primary. The kiosks use a document reader to verify the travel document, and compare biometric data (fingerprints) to validate enrollment. A Global Entry RFID enabled card is issued to U.S. citizen, U.S. Lawful Permanent Resident, and Mexican national Global Entry members (not already enrolled in SENTRI or NEXUS) for use at the NEXUS and SENTRI lanes when entering the U.S. Please note that this card is not valid for use in the NEXUS lanes when traveling into Canada or at the NEXUS or Global Entry kiosks. Global Entry members may use the SENTRI lanes at southern land border ports of entry, provided they travel in a SENTRI registered vehicle and comply with SENTRI requirements. Global Entry members can also use the SENTRI pedestrian lanes

1.4 FAST

The Free and Secure Trade (FAST) program is a Border Accord Initiative between the United States, and Canada designed to ensure security and safety while enhancing the economic prosperity of each country. In developing this program, Canada and the United States have agreed to coordinate, to the maximum extent possible, their commercial processes for clearance of commercial shipments at the border. The program promotes free and secure trade by using common risk-management principles, industry partnership, and advanced technology to improve the efficiency of screening and clearing commercial traffic at our shared borders. With similar goals and techniques, the United States independently administers a version of FAST for low risk imports from Mexico.

Definitions and Terms used in this Handbook

TTP – Trusted Traveler Program – SENTRI, NEXUS, Global Entry and FAST; One of four programs operated by CBP to allow pre-enrolled, low-risk participants to receive expedited border processing, enabling CBP to direct additional scrutiny to the unknown, potentially higher risk, travelers arriving at ports of entry.

VC –Vetting Center – Located in Williston, Vermont. All applications for the Trusted Traveler Programs are vetted by the VC staff before distribution to the Enrollment Centers for further processing. The Director, Field Operations Boston is responsible for the operation of the VC.

3. Eligibility Requirements

3.1 General Eligibility in SENTRI, NEXUS, and Global Entry

Participation in TTPs is voluntary. An applicant may not qualify for participation if:

- The applicant provides false or incomplete information on the application;
- The applicant has been arrested for, or convicted of, any criminal offense or has pending criminal charges or outstanding warrants in any country (the sole exception being for misdemeanor or lesser convictions over 10 years old, in accordance with the Strict Standard);
- The applicant has been found in violation of any customs, immigration, or agriculture regulations, procedures, or laws in any country;
- The applicant is the subject of an investigation by any federal, state, or local law enforcement agency in any country;
- The applicant is inadmissible to the United States under applicable immigration laws or has, at any time, been granted a waiver of inadmissibility or parole;
- The applicant is known or suspected of being or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism; and/or
- The applicant cannot satisfy CBP of his or her low-risk status or meet other program requirements.

Generally, if low-risk status cannot be determined, the application must be denied.

3.2 The Strict Standard for SENTRI, NEXUS, and Global Entry

The standards for vetting NEXUS, SENTRI, and Global Entry applicants include the following:

3.3 SENTRI Criteria for Eligibility

- U.S. citizens and U.S. LPRs.
- Citizens of other countries who are admissible to the United States and are in possession of all required entry documents.
- Must be admissible to the U.S. without a waiver.
- Approved Global Entry and NEXUS members who are in possession of a TTP RFID enabled card may use the SENTRI lanes, provided they are traveling in a SENTRI registered vehicle. Members can also use the SENTRI pedestrian lanes

3.4 NEXUS Criteria for Eligibility

- U.S. citizens and U.S. LPRs who are admissible to Canada and are in possession of all required entry documents.
- Canadian citizens or landed immigrants of Canada who are admissible to the United States and are in possession of all required entry documents.
- Must be admissible to the U.S. without a waiver.
- Approved Global Entry and SENTRI members who are in possession of a TTP RFID enabled card may use the NEXUS lanes entering the U.S. at land border locations, and by sea for small boats.

3.5 Global Entry Criteria for Eligibility

- U.S. citizens and U.S. LPRs.
- Citizens of countries approved for participation through reciprocal bi-national Trusted Traveler arrangements in designated nonimmigrant classifications. These individuals must be admissible to the United States and be in possession of all required entry documents. (Refer to Appendices)
- Must be admissible to the U.S. without a waiver.
- Approved NEXUS members may use Global Entry kiosks, provided their fingerprints and documents are on file.
- Approved SENTRI members who are U.S. citizens or LPRs may use Global Entry kiosks, provided their fingerprints and documents are on file. Mexican nationals approved in SENTRI must apply for Global Entry through GOES, and will be vetted by Mexico. Upon successful vetting by Mexico, Mexican nationals may be approved for Global Entry and use Global Entry kiosks.

3.6 FAST Criteria for Eligibility

- U.S. citizens and U.S. LPRs driving a commercial conveyance into Canada who meet all legal and regulatory requirements (including valid admission documents).
- Canadian citizens or landed immigrants of Canada driving a commercial conveyance into the United States who meet all legal and regulatory requirements (including valid admission documents).
- Mexican citizens or residents driving a commercial conveyance into the United States who meet all legal and regulatory requirements (including valid admission documents).
- Must be 18 years of age or older and possess a valid driver's license.

There are two versions of the FAST Driver program – FAST North and FAST South. FAST participation requirements along the northern and southern border are very similar with minor exceptions.

- For FAST North at the northern border, the driver, carrier, and importer must all participate in the FAST Driver/C-TPAT programs in order to be eligible for FAST processing.
- On the southern border the manufacturer must also be an approved C-TPAT participant.
- FAST North is a bi-national program administered jointly by CBP and CBSA for expedited release into both countries.
- FAST South is administered exclusively by CBP for expedited release into the U.S. only with inbound traffic management assisted by Mexico.

3.7 Records

CBP officers are to determine the relevance of records that are discovered during the vetting process and their connection to the applicant. The mere existence of a record does not mean an applicant should be denied membership. There must be some association of the record to the applicant. Examples of records that may be found, but are not directly connected to the applicant include:



In the case of pending or dismissed charges, certified court records will be required before acceptance into a TTP. The applicant is responsible for providing proof of final disposition. If no disposition is available, then the charges will be treated as a conviction. Dispositions must come from courts or other government sources. Letters from attorneys on behalf of their clients cannot be used to determine a disposition. Court documents will not be required if the disposition is listed in the FBI record.



3.8 Special Considerations Regarding Minors in Trusted Traveler Programs

A child may be enrolled into a TTP even if the parents are not enrolled. However, a parent or guardian must be present at the time of interview of the minor. If the custody of the child is not made clear during the interview, the parent or guardian must provide certified copies of legal documentary evidence of custody. Upon approval, minors (age 17 and under) will not be required to present any further documentation of custodial permission when crossing.

3.9 Commercial Airline Pilots and Vessel Masters

Commercial airline pilots should not be automatically denied membership in a TTP solely on the basis of being listed as the violator in a penalty or fine against a commercial airline. As stated in 19 CFR 122.166, an aircraft pilot is normally culpable for any aircraft violation, and is therefore listed as the violator. This would also be the case for a commercial vessel master or captain in regards to violations against the vessel or conveyance.

3.10 CBP Employee Participation

CBP and other government employees may apply for participation in any TTP as a private citizen. Employee applications will be processed in the same manner as all other applications. Employees pay the same fees as the general public.

4. Applying for Trusted Traveler Programs

4.1 Where to Apply

Persons applying for any of the TTPs should be directed to the CBP website and GOES. On the GOES website, applicants can create accounts, complete the application, and submit fees. Applicants who use GOES will be notified of all decisions regarding the application via his/her GOES account. This includes conditional approvals/notifications to schedule an interview appointment, application approvals and application denials.

5.1 Risk Assessments

All risk assessments for participation in TTPs will be conducted by the VC. CBP officers at the VC will electronically vet each application through the use of automated queries. [REDACTED]

[REDACTED]. These vetting queries include, but are not limited to, the following systems:

Risk Assessment Queries


* Required for SENTRI vehicles. For other programs, queries will be run if the information is available.

Other systems checks may be conducted on a case-by-case basis and include, but are not limited to:



5.2 Risk Assessment Worksheet

The RAW is generated by the vetting officer and includes the vetting queries conducted at the VC. The RAW is attached to the biographic details section of an applicant's summary page in GES. A RAW must be completed for every application.



When interviewing the applicant, officers will ask the applicant to clarify, address or explain the issues noted in the RAW [REDACTED]

If the issue(s) are resolved, the interviewing officer must annotate the resolution in the comment section in the biographic details link in GES.

5.3 Supervisory Discretion at the Vetting Center



5.4 Vetting Status

The “Vetting Status” box reflects the decision of the VC supervisor, which may override the recommendation of the vetting officer.

5.5 Criminality

During the vetting process, a criminal history biographic check is conducted on applicants. [REDACTED] If criminal history is discovered and the applicant appears to be ineligible for the program, the VC will conditionally approve the application and the RAW will be annotated “POTENTIALLY HIGH RISK.” This is specific to III results only. The VC is not restricted from denying the application for criminality if the information is obtained from other than III. This indicates to the EC officer that particularly close attention should be paid to the criminal history. The EC officer must review the criminality and request that the applicant obtain court documents as necessary/relevant. Applicants can only be denied program membership on criminal grounds discovered through a query of III after fingerprints are submitted to IAFIS for biometric verification, unless the criminal history is disclosed on the application.

5.6 Denials after Risk Assessments

External Comments in GES:

Denial notifications are automatically generated by GES and posted in the applicant's GOES account. The denial reasons included in the letter are taken from the "Printed Reasons" box in GES. This information will be provided to the applicant. Denial reasons must be sufficiently explained so they are apparent to the reader. For example, "Applicant denied based on criminal history: Conviction for Armed Robbery in 1997" or "Denied for CBP violation, undeclared mangos in 1997" are acceptable comments. [REDACTED]

Internal Comments in GES:

It is important that denial reasons are clearly articulated in the "Reasons, For Internal Use Only" section in GES. The reasons for a denial must be sufficiently articulated so that someone unfamiliar with the case is able to understand the denial reason(s). [REDACTED]

Once the VC denies an application during the risk assessment, the decision is final and not subject to review by an EC. However, when an applicant contacts the EC seeking an "appeal" or reason for the denial, the applicant should be provided the printed reason for denial. If the applicant claims the actual information used for the denial is incorrect the applicant should be instructed to write a letter to the Ombudsman explaining why he/she feels that the information is incorrect and provide additional pertinent information (e.g., denial letter stated a customs violation in 1997, but the applicant claims he/she has never been the subject of a customs violation).

5.7 GOES Denial Letters

GES automatically generates an electronic notification to applicants who fail the application vetting process. The notification is posted to the applicant's GOES account.

The denial letters contain the following information:

- Date of letter;
- Name and address of applicant;
- PASS ID; and
- A clear, concise statement as to why the applicant was denied. This statement will include such information as: "CBP violation –El Paso, TX, 1997 or Agriculture violation – undeclared fruit, El Paso, TX, 2003, etc." If the denial is due to criminal conviction and/or arrest, the type of offense, year, and state in which the incident occurred will be revealed such as "Conviction/Arrest - DUI, Florida, 2009."

Denial letter comments are for the applicant and provide the reason for denial. The reasons must be clear, concise, and complete. Additional information must be entered into the comment section for those instances where more information, such as the date, location, and type of offense or conviction can be provided. The applicant should be provided with as much information on the denial as possible, in an effort to prevent frivolous letters to the Ombudsman.

Applicants who fail to meet the eligibility requirements after VC vetting will be denied. A notice of denial will be sent to the applicant's GOES account or sent to the applicant by mail.



Denial Code	Reason Code and Explanation
[Redacted Table Content]	

Additional information must be recorded in the comment section in those instances where additional information is needed, such as the date, location, and type of offense or conviction so the final notice sent to the applicant will include the type of offense/conviction and date the offense occurred or the date of conviction. Information that cannot be disclosed includes, but is not limited to, the subject and/or details of current investigations, closed investigations, terrorist-related records, or records belonging to other agencies.



5.8 Approved Risk Assessments

When the risk assessment has been successfully completed (no disqualifying derogatory information found), the applicant's record in GES will be updated to "conditionally approved". In the case of applicants to NEXUS and FAST North, an electronic data share between Canada and the United States will automatically update GEC, GES, and the corresponding Canadian FAST system when either country makes a decision. An applicant who mailed in an application will receive a letter with instructions for scheduling an interview. Applicants who submitted an application through GOES will receive a notice in their GOES account to schedule an interview. Applicants may utilize GOES or call an EC to schedule an interview. Walk-in interviews should be accommodated when feasible.

5.9 24 Hour Vetting

On a recurrent basis, the GES database sends biographic data of conditionally approved applicants and approved members for vetting to check for subject records, wants, and warrants. [REDACTED] are returned for review and adjudication. [REDACTED]

It is the responsibility of the VC supervisor to assign a CBP officer to review the results of the checks against all active enrollees in the GES database daily. [REDACTED]

When it is determined that the member or conditionally approved applicant is not a match to the record being vetted, the [REDACTED]

To: DASGUPTA, RIDDHI [REDACTED]
From: ACOSTA, PETE R
Sent: Tue 2/4/2020 12:49:06 PM (UTC-05:00)
Subject: FW: Green Light Law

A: The NY Green Light law would prevent CBP from receiving information relating to criminal convictions involving motor vehicles (DWIs, misdemeanors or felonies). Membership in a CBP Trusted Traveler Program requires application of strict standards for multiple convictions that can longer be assessed for applicants residing in the State of NY. NCIC III responses from the state of NY currently return an FBI number with no arrest information and states “our files contain no criminal history information for this individual”, but the FBI number validates existence of an arrest history.

Example posted below:

2 of 202/01/20 11:55:21 EST[REDACTED]Nlets

09:55 02/01/2020[REDACTED]
09:55 02/01/2020[REDACTED]
[REDACTED]

***** CRIMINAL HISTORY RECORD *****

***** Introduction *****

This rap sheet was produced in response to the following request:

FBI Number

State Id Number

Request Id

Purpose Code

Attention

The information in this rap sheet is subject to the following caveats:

***** IDENTIFICATION *****

Subject Description

Blank

***** CRIMINAL HISTORY *****

***** INDEX OF AGENCIES *****

* * * END OF RECORD * * *

YOUR REQUEST FOR THE ABOVE CRIMINAL HISTORY INFORMATION HAS BEEN RECEIVED. OUR FILES CONTAIN NO CRIMINAL HISTORY INFORMATION FOR THIS INDIVIDUAL.</NLETS>

From: LAGVILAVA, TAMARI (OCC) [REDACTED]
Sent: Tuesday, February 4, 2020 12:15 PM
To: ACOSTA, PETE R [REDACTED]
Cc: STEVENS, DONALD R (OCC) [REDACTED]
Subject: RE: Green Light Law

Thank you, Pete – I am going to copy you on the email to him. Donald and I are happy to join as well.

Tamari J. Lagvilava
Attorney (Enforcement & Operations)
Office of Chief Counsel

This document, and any attachment(s), may contain information which is law enforcement sensitive, attorney-client privileged, attorney work-product, and/or U.S. Government information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please consult with the CBP Office of the Chief Counsel before disclosing any information contained in this message or any attachment(s).

From: ACOSTA, PETE R [REDACTED]
Sent: Tuesday, February 4, 2020 12:13 PM
To: LAGVILAVA, TAMARI (OCC) [REDACTED]
Cc: STEVENS, DONALD R (OCC) [REDACTED]
Subject: RE: Green Light Law

Tamari,

Sure; I just tried to call but couldn't reach him.

Any time is good.

Pete

From: LAGVILAVA, TAMARI (OCC) [REDACTED]
Sent: Tuesday, February 4, 2020 12:10 PM
To: ACOSTA, PETE R [REDACTED]
Cc: STEVENS, DONALD R (OCC) [REDACTED]
Subject: FW: Green Light Law

Hi Pete – Deputy General Counsel at OGC HQ, Sohan Dasgupta, has asked to connect with OFO to discuss the impact of the New York DMV law on the Global Entry process from the operational perspective. Would you be available for a call this afternoon? I am assuming that he will want to schedule the call as soon as possible.

Thank you,
Tamari

Tamari J. Lagvilava
Attorney (Enforcement & Operations)
Office of Chief Counsel
U.S. Customs and Border Protection
[REDACTED]

This document, and any attachment(s), may contain information which is law enforcement sensitive, attorney-client privileged, attorney work-product, and/or U.S. Government information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please consult with the CBP Office of the Chief Counsel before disclosing any information contained in this message or any attachment(s).

From: COUREY, MARC BENNETT (OCC) [REDACTED]
Sent: Tuesday, February 4, 2020 11:54 AM
To: LAGVILAVA, TAMARI (OCC) [REDACTED]
Cc: KESSLER, LESLEYANNE (OCC) [REDACTED]; STEVENS, DONALD R (OCC)
[REDACTED]
Subject: Green Light Law

Tamari — Can you please help connect Sohan with an operational client, presumably on a phone call on which we'd join the client? Sohan's note is below.

“Sir—who's an operations person at CBP we can talk to about the green light thing? It'll help FO and us.”

I'm about to depart Atlanta, otherwise would join. Perhaps Lesleyanne can join you. Thanks!

Bennett Courey

DHSGLL063

**** Attorney Work Product / Attorney-Client Privileged ****